SecurityExpressions Server User Guide

symantec.

Table Of Contents

Contacting Us

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA

http://www.symantec.com

Technical Support

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

Contacting Technical Support

Customers with a current maintenance agreement may contact Technical Support at altiris.support@symantec.com.

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
    - Error messages and log files
    - Troubleshooting that was performed before contacting Symantec
    - Recent software configuration changes and network changes

Other Products

SecurityExpressions Console

This product enables you to quickly and effectively lock down Windows systems using guidelines similar to ones established by Microsoft, NSA, SANS, and others. Use it to verify the security settings on local and remote systems across your enterprise.

See how well your systems are protected by comparing their current configuration against the Microsoft Security White Paper. A scheduled task mode allows you to compare hundreds of computers at once, then automatically apply fixes interactively or automatically. A sophisticated searching language allows you to catch errors and inconsistencies across your entire network. Printing and reporting capabilities allow you to save output for historical review.

Overview

About SecurityExpressions Audit & Compliance Server

SecurityExpressions Audit & Compliance Server is a Web-based application that runs on a server with Microsoft IIS and an ASP.NET infrastructure installed. From a Web browser on any computer, you can securely perform most audit and compliance functions, such as audit scheduling, reporting, and browsing audit results. The server automatically updates time-sensitive audit policies such as patch, antivirus, and vulnerabilities. The Web pages interact with a central database and a service that performs the auditing.

The server offers three ways to audit:

Self-service audits

Audit-on-Connect

Audit-on-Schedule

Self-Service Audit

What is Self-Service Auditing?

Self-service auditing lets anyone audit just their local Windows computer. Typically, a person performing self-service audits is not a SecurityExpressions user, but must have administrator privileges on the computer they're auditing. A designated Web page gives self-service auditors access to self-service features only.

A self-service audit runs a local system audit against a policy and then allows you to view the resulting system assessment. You can audit, assess, and, comply with your organization's unique security policy or a standard policy file. A self-service audit may require the acceptance of a corporate agreement.

Self-service audits can optionally apply settings defined in an Audit-On-Connect scope. If a self-service audit uses an Audit-On-Connect scope, it does so to audit just the local system. The other devices in the scope are ignored.

Self-Service Audit Agreement

An organization may require the acceptance of corporate agreement text before allowing an audit. Your organization can customize an agreement and include it in the Self-Service Audit settings. The administrator configures the system to require users to accept the agreement text before running a self-service audit or skip this agreement.

If you wish to comply with the agreement text, the Self-Service Audit proceeds and the results display. If you disagree with the agreement, the self-service audit does not occur.

Agreement acceptance remains throughout the session. If you time out or shut down, you must accept or reject the agreement the next time you want to audit the local system.

The agreement version number logs the user's acceptance of the agreement.

How to Audit your Local Computer

Self-service audits are for auditing Windows computers only.

To perform a Self-Service Audit:

1. From the server application's home page, click the **Self-Service Audit** link at the bottom of the page. You may also reach the Self-Service Audit page by browsing to **https://*servername*/seserver/selfservice**, where *servername* is the name of the server on which the server software resides.

   If agreement text was configured, you must accept the agreement to continue.

2. Select a method of self-service auditing by clicking one of the following links.

   - **Self-audit using a specific policy file -** Click this link to select from a list of policy files.

   In order for the list to contain policy files, the administrator of this product must have already created policies and associated policy files with them. If the Policy File list is empty, ask the product's administrator to create some policies.

   - **Self-audit against a list of policy files that apply to your computer -** Click this link to self audit based on an Audit-on-Connect scope, which has the ability to

check your system against several policy files during one audit. If the administrator of this product created an Audit-on-Connect scope that contains your system, you may use this method to start an audit on your system. Audit results are automatically recorded for review and reporting.


If the administrator of this product did not create an Audit-on-Connect scope that contains your system, you can only select **Self-audit using a specific policy file**.

3. A security warning appears, alerting you that you need to install WebAudit before you proceed with the self-service audit. Click **Yes** to install WebAudit.

WebAudit is an ActiveX component required for self-service auditing. It remains in the browser's cache, so you won't need to install it again unless you clear the cache and then perform another self-service audit.


You cannot perform a self-service audit without this component. If you click **No**, you won't be able to complete the audit.

4. If you clicked **Self-audit using a specific policy file** on the Audit Your Local System page, select a policy file from the Use this Policy File list. Then click **Audit Now** to perform the self audit.

The audit compares this policy file against your system.

5. If a Permit Server Audit message appears, click the **Yes** button to continue.

If you clicked **Self-audit using a specific policy file** on the Audit Your Local System page, the audit results display directly on the page. Click a rule link in the Description column to learn more about that rule. You may use the button bar to perform operations on the audit results.


If you clicked **Self-audit against a list of policy files that apply to your computer** on the Audit Your Local System page, only a cumulative posture result displays on the page. No detailed audit results appear.

Configure Servers

About Server Configuration

Before you can audit systems using the server application, you must configure server settings. From fundamental settings such as database connection and policy-file-library synchronization to specific settings that drive scheduled and Audit-on-Connect, the Settings tab provides a central location for configuring the server.

To access the Settings tab, click **Configure Servers** on the application's home page. Use the links at the top of the tab to open the various settings pages.

Local Server Settings

Local Settings include parameters of individual audit servers. Most settings are global to all servers in the system, but the Local Settings apply only to one named audit server. The heading, such as **Local Settings are for Server: ENTERPRISEHOST** indicates that the displayed settings are for the server named ENTERPRISEHOST. The database server and database name also appear.

About User Roles

If the tasks involved in auditing computers for security compliance are divided among different people in your organization, we recommend establishing *user roles* to control who can use different features in this application. Several key pages contain settings that let only members of specified Windows User Groups access certain pages and their features. This allows each user to focus on their tasks while preventing unauthorized users from performing restricted operations. For example, administrators of the product need access to all pages including configuration pages, but auditors only need access to pages used for setting up audits and viewing results.

Tip: Create Windows User Groups based on the access level you plan to grant different users of the application. Then assign these groups to the corresponding pages.

Pages with Role Settings

You establish user roles by entering Windows Group Access settings on the following pages in the application. You may restrict access to the pages or features themselves, plus the reports and audit results based on the restricted machine lists, policies, scopes, and scheduled tasks.

Page Access

Machine List Access

Policies

Scopes

My Machine Lists

Scheduled Tasks

Viewing Audit Results

SecurityExpressions generates audit results through the following kinds of audits. To view results from each kind of audit, a user needs rights to view results from key configurable items (machine lists, policies, and scopes) involved in the audit. The configurable items to which a user needs audit-result viewing rights, for each kind of audit, are:

Audit on Schedule

- policies
- My Machine Lists or global machine lists

Audit on Connect

- policies
- scopes

Self-Service Audits

- policies
- any My Machine Lists or global machine lists the computer belongs to, whether or not the machine list is involved in the audit
- Super User item rights, if the computer does not belong to any machine list

Instant Audits - performed in the console application's Audit tab

- policies
- global machine lists, if auditing a machine list
- any My Machine Lists or global machine lists that the computer(s) belong to, if auditing individual computers instead of a machine list
- Super User item rights, if the computer does not belong to any machine list

Web-Services Audits - audits activated through the Web-services layer (see the *SecurityExpressions Web Services API Guide* for more information)

- policies
- global machine lists, if auditing a machine list
- any My Machine Lists or global machine lists that the computer(s) belong to, if auditing individual computers instead of a machine list
- Super User item rights, if the computer does not belong to any machine list

Setup Page

Database Connection

The Application Setup page displays the name of the system where the database resides and the database's name. The Database Connection settings on the Application Setup page let you connect the SecurityExpressions Audit & Compliance Server to a central database.

If you don’t want to connect to an existing database and don’t need to create a custom database, you have the option of creating the database using the Database Connection settings instead of creating it in the database application.

We recommend you don't use SQL Server's master database as the SecurityExpressions database.

To establish a valid database connection:

1. In the Database Type drop-down list, select the manufacturer of the database software you use.
2. In the Database Server Name box, type the name of the computer containing the database software you use.

   If you're not connecting to the default instance of the database, enter the server name in *computername**databaseinstance* format.

3. In the Catalog (Database) Name box, type the name of the database you want the server software to connect to or create.
4. If you want to create a database instead of connecting to an existing database, check **Create**.
5. Decide if you want the server application to use SQL Server or Windows authentication to log in to the database.

   The application uses the credentials typed in the Database Login and Database Password boxes for all users every time they open the application. You can enter the credentials of any account that has read/write access to the database and tables.

   - If using SQL Server authentication, type a SQL Server account's user name and password in the Database Login and Database Password boxes.
   - If using Windows authentication, check **Use Windows Authentication** and type a Windows account's user name and password in the Database Login and Database Password boxes.

   This sets the application and all related services to run under this account, including ASP.NET. To increase security, you can create a domain user with limited network access and read/write access to the database, and then use that account's credentials.

   If both the server application and the database are on the same computer, then the you can use the ASP.NET account's credentials. To do this, grant the ASP.NET user permission to use the database in the database software. Then type **.\ASPNET** in the Database Login box and leave the Database Password box blank.

6. Click **Apply**.

Make sure to connect all server applications you install in the organization to this database.

Secure Connection

In order to establish a secure connection to the server-software Web site, whether you're accessing it from the system on which you installed the software or remotely from another system, you must use Secure Sockets Layer (SSL). That means you must include HTTPS in the URL. Use the format *https://<hostname>/seserver*, where *<hostname>* is name of the system containing the server software.

Windows 2000 Servers

If you installed the server software on a Windows 2000 Server system running IIS, you must configure SSL by setting up the server certificate on that system.

If the system on which you installed the server software is not running Windows 2000 Server, skip this procedure.

1. On the Windows 2000 server, open Control Panel and double-click **Administrative Tools** and then **Internet Information Services** to open the IIS Administrative Panel.
2. In the Web Site folder, right-click **Default Web Site** and choose **Properties**.
3. On the **Directory Security** tab, in the Secure communications section, click **Server Certificate**.
4. Click **Next** in the Wizard. On the second page of the Wizard, select **Assign an existing certificate**.
5. In **Available Certificates**, select the SecurityExpressions Audit & Compliance Server Certificate.
6. Finish the Wizard.
7. Click **OK** on the **Default Web Site Properties** window.

Now you are ready to access the site using SSL.

Credential Store User

The Credential Store User settings on the Application Setup page let you create and log in to credential stores. Stored credentials are a way for a user with the proper credentials to give a user without them the access needed to audit the target systems without actually revealing the credentials. A credential store is a place in the database where you can save the credentials in encrypted form. Auditors can use the credentials without seeing what they are. Security is not compromised and the organization has the flexibility to assign auditing duties to someone without top security credentials.

When an audit begins, it obtains the credentials of each target computer from the credential store selected in the Credential Store User section of the Application Setup page. If it does not find these credentials, it looks for credentials delegated from the console application.

You must configure a credential store for the application to log in to every time someone uses the application. On the SecurityExpressions Audit & Compliance Server, you can create new Credential Stores on the Application Setup page or use Credential Stores previously created from the SecurityExpressions Console.

If you haven't created any credential stores in the console application that you can log in to, you need to create a credential store first.

To log in to a credential store:

1. In the Credential Store Name box, select the credential store's user name.
2. In the Credential Store Password box, type the credential store's password.
3. Click **Apply**.

All servers connected to the same database must use the same credential store.

Creating Credential Stores

You must configure a credential store for the application to log in to every time someone uses the application. You can either create a credential store in the server application or use a credential store created in SecurityExpressions Console. Each group of SecurityExpressions Audit & Compliance Servers will have its own Credential Store.

Once you create a credential store, you can't modify it.

To create a credential store:

1. In the Application Setup page, click **Add New**.
2. In the New Credential Store User Name box, type a user name for logging in to this credential store.
3. **Optional:** In the New Credential Store User Full Name box, type a descriptive name.
4. **Optional:** In the New Credential Store User Description box, type any information about this credential store other users might find helpful.
5. In the New Credential Store User Password box, type a password for logging in to this credential store.
6. In the Verify Credential Store User Password box, type the password again.
7. Click **Update**.

SecurityExpressions Console Credential Stores

When you create a Credential Store in the SecurityExpressions Console, you create a container that securely saves all of your machine list and host (target system) credentials in the database. After you create the credential store, you can delegate the credentials to the Audit & Compliance Server. This allows users belonging to certain Windows Groups to perform operations using the delegated credentials without knowing or seeing the credentials.

Software Registration

The Software Registration options on the Application Setup page let you register the software for use. You must enter a valid license key in order to activate the server application. If you purchased the Audit-on-Connect component, you must activate that feature with a second license key.

To register the software:

1. In the SecurityExpressions Audit and Compliance Server License Key box, enter the license key for general use of the application.
2. If you purchased Audit-on-Connect, in the SecurityExpressions Audit-on-Connect License Key box, enter the license key for that component.
3. Click **Apply**.

Site Preferences

The Site Preference options on the Application Setup page let you select general settings for the application. Click **Apply** after changing these settings.

Enable Web Services

Select this check box to enable SecurityExpressions' Web-services layer. To learn more about the Web-services layer, see *SecurityExpressions Web Services API guide*, included in your installation package.

Allow Remediation

Select this check box to allow Web-services remediation functions to apply fixes to computers audited through Web services.

Session Duration

Session duration is a time-out period that sets the maximum number of minutes for a Web session. The session lasts until this time passes or a different Browser accesses the server. When the session expires, local session information, including authentication, is lost. Many settings, once initialized, remain through the session duration.

Once you open a new Browser, the session duration resets to the configured time period.

Maximum number of simultaneous audits for Audit-on-Connect

Simultaneous audits affect network capacity and speed. If you find the default number of simultaneous Audit-on-Connect audits consumes too many CPU and network resources, change this setting to a smaller number until you find the right balance.

Maximum number of simultaneous audits for Audit-on-Schedule

Simultaneous audits affect network capacity and speed. If you find the default number of simultaneous Audit-on-Schedule audits consumes too many CPU and network resources, change this setting to a smaller number until you find the right balance.

Do not use more than __ Mbps (megabits per second) of bandwidth

To control the amount of network bandwidth the software uses during an audit, select this check box and type the maximum number of megabits per second of bandwidth you want audits to consume. The less bandwidth allotted to audits, the longer audits will take to complete. You must enter a number between 0.01 and 10,000.0.

Other Servers Local Settings

Other servers in the System on the Application Setup page lists the other servers in this system that use the central database. When you click a link, you view the Local Settings page for those servers, but only one server is available to view at a time. By navigating to the local settings for each individual server, you can change the local settings on all servers in the system from one location.

All settings other than those on the Setup page are shared across all servers using the same database.

Page Access

Page Access identifies who has access to each SecurityExpressions Audit & Compliance Web page, including the Home and Self-Service Audit pages. For each page, type the name of a Windows User Group that you want to grant access to the page. You cannot enter individual users. Any user belonging to that Group has access, while users who do not belong to the group are denied access.

To allow all users to access a page, type **Everyone**. To prevent all users from accessing a page, type **None**.

If you enter multiple Windows groups, separate them with commas. If a Windows User Group isn't on the local computer, you'll need to enter the group in *domain**groupname* format.

Tip: Before making Group assignments to a specific page, become familiar with Windows Users and Groups in your organization. To see the current Users and Groups, open Control Panel and double-click the **Administrative** icon. Then open **Computer Management** and view **Local Users and Groups**.

Item Rights

The Item Rights options, found on the Page Access page, let you list which Windows User Groups are allowed to do the following:

Edit Private Items

Allow others to modify items that are normally exclusive to the user who created them, such as My Machine Lists and scheduled tasks.

Miscellaneous Target

Usually, the View Audit Results setting for scopes and machine lists controls access to most audit results, since most audits involve a scope or machine list. In the rare cases where 1) an audit doesn't involve a scope (computer audited individually) and 2) the computer isn't part of any machine list (whether or not a machine list was used in the audit), access to the audit results are controlled with this setting instead. Users with this right can view results from these kinds of audits.

Possible cases include the following, only when the computers audited don't belong to any machine list:

- self-service audits
- instant audits performed in the console application's Audit tab, not using a machine list
- audits activated through the Web-services layer not using a machine list (see the SecurityExpressions Web Services API Guide for more information)

Remediate Miscellaneous Targets

Usually, the View Audit Results setting for scopes and machine lists controls access to most audit results, and therefore remediation of audit results, since most audits involve a scope or machine list. In the rare cases where 1) an audit doesn't involve a scope (computer audited individually) and 2) the computer isn't part of any machine list (whether or not a machine list was used in the audit), access to the audit results are controlled with this setting instead. Users with this right can view results from these kinds of audits.

Possible cases include the following, only when the computers audited don't belong to any machine list:

- self-service audits
- instant audits performed in the console application's Audit tab, not using a machine list
- audits activated through the Web-services layer not using a machine list (see *SecurityExpressions Web Services API Guide* for more information)

Super User Access

Administrators of the product need to modify all configurable items (scopes, scheduled tasks, etc.)and view audit results, whether or not they're listed in the Windows User Groups with access to a configurable item or its audit results, and regardless of who owns private items such as My Machine Lists and scheduled tasks. We recommend entering a Windows User Group consisting of all product administrators here to ensure they're never locked out of audit results, configurable items, and private items.

Global Machine List Access: User Roles

When you schedule an audit, you can specify which computers to audit by selecting machine lists created on the My Machine Lists page and machine lists created in the console application (global machine lists). You can grant or restrict access to My Machine Lists and the results from audits using them with the Windows Group Access options on the My Machine Lists page. Since global machine lists were created in the console application, the server application needs to provide a place to grant or restrict access to them and the results from audits using them. The ML Access page is where you can accomplish that.

If the central database doesn't contain any global machine lists created in the console application, the table on this page will be empty.

To grant or restrict access to a global machine list in the Audit and Compliance Server:

1. Click the machine list's name in the Name column.
2. Set Windows Group Access. Enter Windows groups, separated by a comma, that can use this machine list, remediate computers in this machine list, and view audit results for this machine list. This establishes which users can access this machine list and its audit results due to their role. If a Windows User Group isn't on the local computer, you'll need to enter the group in *domain**groupname* format.
    - In the Use Machine List field, enter the Windows groups who should be able to modify the machine list.
    - In the Remediate field, enter the Windows groups who should be able to remediate computers in the machine list.
    - In the View Audit Results field, enter the Windows groups who should be able to view results from audits using the machine list.

    To grant all users access, type **Everyone**. To restrict all users, type **None**.
3. When you're done, click the **Add/Update** button.

Policy File Library

Before you can select a policy file in the Policies page, you must enter the policy file library's path and credentials here. This enables the application to gain access to the library and its policy files.

To gain access to a policy file library:

1. In the Library URL field, enter the library's path.
2. In the Library Login field, type the user name needed to gain access to the library.
3. In the Library Password field, type the password needed to gain access to the library.

Library Synchronization

Policy files are updated frequently by the organizations that issue them. If you audit with policy files from a standard policy library, such as the policy file library found at http://www.pedestal.com/products/se/resources/Library, you might want to set a synchronization schedule to remain current. This keeps audits in compliance with current policy files.

To synchronize with a Policy File Library:

1. Check the **Synchronize with a policy file library** box.
2. Decide whether to check for policy file updates regularly on a schedule or to just update now.

To check for frequent policy file updates, you may choose to **Check for policy file updates** during a specific time period (days, minutes, hours). If updates exist, they will be downloaded for the SecurityExpressions Audit & Compliance Server to use.

Check Now updates the policy files immediately.

3. Click **Update** to store the policy file library configuration. The settings are stored but can be modified.

About Policy Files

Security policies lay a solid foundation for the development and implementation of secure practices within an organization. In SecurityExpressions, policy files contain the rules to which an organization must adhere for their system security configuration. Compliance with policies requires an understanding by staff of not only the individual policies but also of the circumstances in which such compliance is expected in their daily activities. Policy files have a .SIF extension.

A high-level security policy may outline specific requirements or rules that must be met, such as the rules and regulations for appropriate use of the computing facilities. A technical standard or configuration guideline is typically a collection of system-specific or procedural-specific requirements that everyone must meet. For example, you might have a standard that describes how to harden a Windows workstation for placement on an external network (DMZ). Administrators must follow this standard exactly if they wish to install a Windows 2003 workstation on an external network segment.

The Security Policy File Library provides pre-defined and customizable system security policy files and security guidelines from well-known sources, such as Microsoft, SANS, NSA, NIST, CIS, as well as policy files including Microsoft Patches, user settings, and Solaris patch management. You can select a policy file to use or modify for your audits.

How System Scores are Calculated

The score a system gets from an audit is calculated using the properties of rules checked against the system during the audit. The properties used are:

Rule Result - Each rule returns a result of OK, Not OK, Error, or Info during an audit. Rules that return Info or Error are not included in the calculation.

Weight Values - Each rule is assigned a weight value from one of the three rule keys, in this order: Weight, Impact, or Priority. The Weight key is not a key that each rule automatically has; it must be created by a user.

If a Weight key exists for a rule and has a value, it always becomes the rule's weight value. If there is no Weight key, the rule gets its weight from the Impact key. If neither key has a value, then the rule gets its weight from the Priority key. If none of these keys have a value, the rule gets a weight value of 1.0.


You can customize the values of rules in one of two places:
1. In the SecurityExpressions server interface by editing the policy file and then uploading it into a policy.
2. In the SecurityExpressions console application, if using it, by adjusting rule keys in the .SIF file.

The following is the formula the software uses to calculate system scores:

(weighted total of OK results ÷ (weighted total of OK rules + weighted total of Not OK rules)) × 100

Example

An audit contains four rules:

- 1 High Priority
- 1 Medium Priority
- 1 Low Priority
- 1 no priority or impact, and no Weight key exists

The weight values are:

- High:1.5
- Medium:1.0
- Low:0.5

The rule with no priority or impact set assumes a weight of 1.0, which happens to also be the default Medium priority weight in this example. If none of the rules return Info or Error, the weighted total of all rules is:

$$((1 \times 1.5) + (1 \times 1.0) + (1 \times 0.5) + (1 \times 1.0) + 0) = 4.0$$

So, if the high-priority rule returns Not OK and the other three rules return OK, the score will be the actual weighted total for OK rule results [i.e. (1×1.0)+(1×0.5)+(1×1.0)] divided by the weighted total of all rules [i.e. 4.0], multiplied by 100:

$$2.5 \div 4.0 \times 100 = 63$$

Target Options

The Agent & Service Configuration options are for Windows target systems only. The SSH Agent Authentication options are for UNIX target systems only.

Agent & Service Configuration

The Agent & Service Configuration options let you manage the remote execution of scripts and programs.

Default method for remote execution on Windows

When a method for executing scripts and programs is not explicitly given in a rule or security check, the application uses the method selected. When set to Automatic, the application tries to run executables using all other methods until it finds a compatible method. It tries the methods in this order:

1. Task Scheduler - Uses the Windows Task Scheduler to remotely execute scripts and programs.
2. WMI - Uses Windows Management Instrumentation, which is typically enabled on all Windows platforms, to remotely execute scripts and programs.

3. Agent - Uses the audit agent to remotely execute scripts and programs. Before auditing, make sure to install the agent on the remote computer or check the **Automatically install Agent if required in order to execute scripts and programs remotely** box.

Automatically install Agent if required to execute scripts and programs remotely

Check this box to automatically install the agent on the remote system when the agent is necessary to complete an audit. The agent can only be automatically installed on Windows systems. For UNIX systems, you must install the agent manually. If you select either Agent or Automatic from the Default method for remote execution on Windows drop-down list, consider checking this box.

If required services are not started, start them before auditing and stop them after audit completes

Check this box to start whichever service the selected remote-execution method needs, such as WMI or the Windows Task Scheduler, before auditing and stop the service after the audit completes. Starting and stopping the service if it's not already running ensures that the audit will not fail.

SSH Agent Authentication

When performing Audit-on-Connect audits, the server software can communicate with UNIX computers through the audit agent or through SSH. When performing Audit-on-Connect audits through SSH, you can authenticate users by either setting up password-based authentication on the Scopes page or uploading private keys to the server application. Use the SSH Agent Authentication section of the Agent & Service Configuration page to set up SSH private keys.

 The SSH Agent Authentication options apply to Audit-on-Connect audits only.

To upload a new SSH key:

1. Click **Browse** to locate and select the private key file.
2. In the Key Password box, type in the Password box the passcode associated with the private key file.
3. Click **Add New**. The key and passcode appear in the table.

You can add keys in any order. When Audit-on-Connect attempts to connect to a UNIX computer, it checks all keys in the list to see if any of them work.

To edit an existing SSH Key:

1. Click the **Edit** hyperlink for the SSH key that appears in the table.
2. Browse for a new key file and type the passcode associated with the key file.
3. Click **Update**.

To delete an existing SSH Key:

1. Click the **Delete** hyperlink for the SSH key that appears in the table.

   When you delete an SSH key, you remove it from the database. A warning appears to remind you that you are about to remove the key from the database.

2. Click **Delete** to remove the SSH key.

Database Cleanup

The database stores data about audits, as well as console and server events. You might decide that it is unnecessary to use database space to retain this data permanently. The Database Cleanup settings allow you to automatically delete data from the database on a schedule. You can also use the Clean Now button to perform an unscheduled cleanup.

Cleanups delete data generated by any console or server application connected to the same database, not just the server application executing a cleanup. They also clean up data generated by Web services, the COM object, and the command line.

Event-log cleanups and audit-data cleanup tasks are scheduled and run independently from each other.

Event Log Settings

SecurityExpressions retains a log of console and server events that it stores in the database.

Perform daily discard of event log data older than __ days

To clean up the event log, check this box and type the number of days for which you want to retain data before deleting it. Then click **Update**. Log entries are automatically cleaned up at 2 a.m.

Update

Click this button to update the event-log settings.

Clean Now

Click this button to perform an unscheduled event-log cleanup. Then click **Delete** to confirm the action or **Cancel** to cancel it.

Audit Data Cleanup Tasks

You may create more than one cleanup task. Click **Add New** to create a task. To modify an existing task, locate the task in the table and click the **Edit** link. To delete an existing task, locate the task in the table and click the **Delete** link.

Task Name

Type a name for this cleanup task.

Daily Cleanup

Check **Enabled** to enable this cleanup task.

Audit Results

Select how much audit data you want to retain when cleanups occur. Cleanups occur at 2 a.m. nightly when a cleanup task is enabled.

- **Discard audit data older than __ days** - Type the number of days for which you want to retain data before deleting it.
- **Discard all but most recent audit for each policy and target** - From the drop-down list, select the time span for which you want to keep the most recent audit performed on each policy file you used to audit and on each target audited. The database retains the data from one audit performed on each policy file and each

target for every week, month, year, or overall.

If you select Yearly, for example, the database will retain the last audit performed on every policy file and on every target audited for every year you've audited using this database. Because cleanups occur nightly, the last audit saved during the current year could potentially change nightly until the year ends. If you select Overall, however, only the most recent audit performed on each policy file and on each target remains in the database after each nightly cleanup.

The application recognizes the span of a week to be when weeks are configured to start and end in the database.

- **Discard audits older than __ days that failed to run or had errors only** - Cleanup occurs only to data from audits that failed to run or audits where all rules had Error ratings. Type the number of days for which you want to retain data before deleting it.

Audit Types

If you want to clean up audit data generated from certain audit types only, check the boxes next to the audit types.

- **Audit-on-Connect and self service** - Cleans up data from only Audit-on-Connect audits and self-service audits.
- **Scheduled** - Cleans up data from only scheduled audits, including audits scheduled in any console application connected to the same database the server application uses. It also includes audits performed through the Web service.
- **Console interactive** - Cleans up data from only audits performed in the console application's Audit tab.
- **COM object and command line** - Cleans up data from only audits performed through the COM object and the command line. Audit results imported through the command line are considered command-line audits regardless of what kind of audit produced the results.

Policies

All policy files (.sif) used to generate audit data in the database are listed. If you want to clean up audit data generated from certain policy files only, check the boxes next to the policy files.

If you leave all boxes unchecked, scheduled cleanups include all policy files listed plus any new policy files used in audits performed after configuring this cleanup task. If you check all boxes, scheduled cleanups include just those policy files.

Add Task

If you're creating a cleanup task, this button appears. Click it to save the options you set as a new cleanup task.

Update Task

If you're modifying an existing cleanup task, this button appears. Click it to update the task with the new settings.

Cancel

Click this button to cancel creating a new cleanup task or modifying an existing cleanup task.

Clean Now

Click this button to perform an unscheduled cleanup on audit data. Then click **Delete** to confirm the action or **Cancel** to cancel it.

Self-Service Audit Agreement

An organization may require the acceptance of corporate agreement text before allowing an audit. Your organization can customize an agreement and include it in the Self-Service Audit settings. The administrator configures the system to require users to accept the agreement text before running a self-service audit or skip this agreement.

If users executing the self-service audit wish to comply with the agreement text, the Self-Service Audit proceeds and the results display. If they disagree with the agreement, the self-service audit does not occur.

Agreement acceptance remains throughout the session. If users time out or shut down, they must accept or reject the agreement the next time they want to audit the local system.

To configure the self-service audit agreement:

1. Click **Use the Following Agreement**.
2. Type the text of the agreement in the scroll box.
3. Type a version number for the agreement in the Agreement Version box.

   If you update the version number each time you modify the agreement, you can keep track of the which version of the agreement is current. Every time a user accepts the agreement, the event is logged with this version number.
4. Click the **Update** button to save the agreement settings.

Agent Downloads

The Agent Downloads page lets you download the installation packages for all audit agents, Windows and UNIX, directly from the Audit and Compliance Server to the computer on which you want to install the agent.

To download an installation package:

1. Click the link corresponding to the platform of the computer on which you want to install the agent.
2. In the File Download dialog box, click **Save**.
3. In the Save As dialog box, browse for the location on the computer where you want to install the agent and click **Save**.
4. When the Download Complete dialog box appears, click **Run** to start the installation process or **Open Folder** to open the location on the computer where you downloaded the installation package.

Site Preferences

The Site Preference options on the Application Setup page let you select general settings for the application. Click **Apply** after changing these settings.

Enable Web Services

Select this check box to enable SecurityExpressions' Web-services layer. To learn more about the Web-services layer, see *SecurityExpressions Web Services API guide*, included in your installation package.

Allow Remediation

Select this check box to allow Web-services remediation functions to apply fixes to computers audited through Web services.

Session Duration

Session duration is a time-out period that sets the maximum number of minutes for a Web session. The session lasts until this time passes or a different Browser accesses the server. When the session expires, local session information, including authentication, is lost. Many settings, once initialized, remain through the session duration.

Once you open a new Browser, the session duration resets to the configured time period.

Maximum number of simultaneous audits for Audit-on-Connect

Simultaneous audits affect network capacity and speed. If you find the default number of simultaneous Audit-on-Connect audits consumes too many CPU and network resources, change this setting to a smaller number until you find the right balance.

Maximum number of simultaneous audits for Audit-on-Schedule

Simultaneous audits affect network capacity and speed. If you find the default number of simultaneous Audit-on-Schedule audits consumes too many CPU and network resources, change this setting to a smaller number until you find the right balance.

Do not use more than __ Mbps (megabits per second) of bandwidth

To control the amount of network bandwidth the software uses during an audit, select this check box and type the maximum number of megabits per second of bandwidth you want audits to consume. The less bandwidth allotted to audits, the longer audits will take to complete. You must enter a number between 0.01 and 10,000.0.

Audit-On-Connect

What is Audit-on-Connect?

Audit-on-Connect is an optional feature of SecurityExpressions Audit & Compliance Server that is sold separately. It enables you to audit systems as they connect to the network rather than on a fixed schedule. This allows you to audit systems that might not be regularly or predictably connected to the network such as field-user laptops. This also allows for systems that are missed in a scheduled audit to be automatically picked up the next time they connect.

Use the following pages to configure Audit-on-Connect:

- Policies
- Scopes
- Notifications
- Exceptions
- Connection Monitors
- Network
- Audit on Connect Tracing

Policies

Policies Page

When you create a new policy, you assign a name and a policy file (.sif) to the policy. Note that policies differ from policy files: a *policy* contains a designated *policy file*.

From the Policies page you create policies to define the audits. You also edit or delete existing policies. If performing an Audit-on-Connect audit, you also set the run-time variables on the Policies page.


Policies are saved to the database. If more than one person is editing the same policy at the same time, the version saved last is the only version that will be stored.

Note that you can associate one or more policy files with specific conditions and the scope.

The Policies table displays available policies for the audits and policy configurations.

Policies Table

The Policies table displays available policies for the audits and policy configurations. The Policies table consists of the following columns:

Column	Description
Active	If Yes, then apply the policy. If the policy is active, within that Scope, the policy will be applied. If No, the policy is not applied but will not be deleted.
Edit	Make changes to this policy entry in the table.
Delete	Remove this entry from the table.
Name	Policy name as it is listed for selection when creating a

	scope or scheduled task.
Description	Optional statement about the policy.
Policy File	Name of the policy file (.sif), from the policy file library or a customized policy file.
Last Updated	Date and time the policy file was last saved to the database.
Configure	Some policy files, such as the NSA Guidelines for Windows XP and Windows 2000, contain a special rule named .CONFIGURE. The .CONFIGURE rule allows you to configure your policy files and set global parameters for policy files at run time. This column shows whether or not the policy file contains the .CONFIGURE rule. Certain information is unique and distinct between systems or groups of systems. A run-time policy variable allows administrators to use a single policy file but allows identification of unique rules that require variable information.
Windows Group Use Access	Specify the Windows User Groups who can use this policy, if you want to restrict access to this policy. Displays "Everyone" if the policy isn't restricted.
Windows Group Remediation Access	Specify the Windows User Groups who can remediate audit results generated using this policy, if you want to restrict access to remediation through this policy. Displays "Everyone" if remediation through this policy isn't restricted.
Windows Group Results Access	Specify the Windows User Groups who can access results from audits that used this policy, if you want to restrict access to this policy's audit results. Displays "Everyone" if the policy's audit results aren't restricted.
Use on Link Type (Audit-On-Connect only)	Specify whether to run this policy over fast or slow connections, or both kinds. Some policies might not be appropriate to run over slow connections if they request a large amount of data. For example, applying large policy files like MS Fixes over a slow network connection, such as a 56K modem, can take a long time.
Device Types (Audit-On-Connect only)	Audit with this policy on these device types. Choices include Windows, UNIX, and Unknown.
Posture Condition (Fail If) (Audit-On-Connect only)	The rules for determining if the resulting posture after auditing with this policy is Pass or Fail. The posture is based on all policy-file rule results (OK, Not OK), plus impact and priority settings. Available posture conditions are: • Always Pass • Any Fail • Any Not OK • Any Not OK with Priority • Any Not OK with Score • Any Not OK with Impact • Any Not OK with Key
Cache Pass For (Audit-On-Connect Only)	Specify how long posture results remain valid when the system passes an audit based on this policy. This is a way

	to control how often a system gets audited — as long as a posture result remains valid, the software won't attempt to audit a system if it connects to the network again. Instead, it returns a posture result of Pass.
Cache Fail For (Audit-On-Connect Only)	Specify how long posture results remain valid when the system fails an audit based on this policy. This is a way to control how often a system gets audited — as long as a posture result remains valid, the software won't attempt to audit a system if it connects to the network again. Instead, it returns a posture result of Fail.

Adding Policies

To create a policy:

1. Click **Add New** on the Policies page.
2. Select a policy file to associate with the policy using one of the following methods.
    - Upload a policy file – Type the name or Browse for a SIF file. If the SIF file is encrypted, type a password in the Password box to decrypt it.
    - Download this file from the Policy File Library – Transfers a copy of a policy file from the Policy File Library over the network. Click the **Choose** button to display a list of the policy files available in the library. Click a policy file to select it.

    This option is available only if the server can access a Policy File Library.
3. Optional: In the Name box, change the name of the policy.

    The name of the policy file you selected in step 2 appeared in this box when you selected it.
4. Optional: In the Description box, type a description of the policy.
5. If you uploaded a policy file that's encrypted, type a password to decrypt it in the Password box.

    Policy files downloaded from the Policy File Library aren't encrypted.
6. If you want the policy to be available to use in audits, check the **Make this policy active** box.

    Clear the check box to make the policy unavailable to use in audits without deleting the policy.
7. Check the **Policy is kept up to date with Policy File Library** box if you want to regularly update the SIF files in this policy using the policy file library available on line.

    This option is available only if the server can access a Policy File Library.
8. If you want the policy to be available to use in self-service audits, check the **Available for use in self-service audits** box.
9. Type a name and optional description of the policy.
10. For Audit-On-Connect include the Link Type, Device Type, Posture Condition, Pass Results Valid For and Fail Results Valid For settings.
11. Set Windows Group Access. Enter Windows groups, separated by a comma, that can use this policy, remediate audit results generated using this policy, and view audit results for this

policy. This establishes which users can access this policy and its audit results due to their role. If a Windows User Group isn't on the local computer, you'll need to enter the group in *domain**groupname* format.

- In the Use Policy field, enter the Windows groups who should be able to modify the policy.
- In the Remediate field, enter the Windows groups who should be able to remediate audit results generated using this policy.
- In the View Audit Results field, enter the Windows groups who should be able to view results from audits using the policy.

To grant all users access, type **Everyone**. To restrict all users, type **None**.

12. Click **Add Policy** to revise the policy settings in the database.

Some policy files display a Policy Configuration box at this point. If the Policy Configuration box appears, select the configuration settings in the box. Then click **Add Policy** again.

Now you may base audits on this policy when setting up Audit-on-Connect or Audit-on-Schedule.

Editing Policies

When editing a policy, you can modify any policy characteristics. For example, by clearing the **Make this policy active** check mark, that policy no longer applies for the Scope. You could also change the policy by selecting a previously saved file or uploading a policy file from our Web site.

Policies are saved to the database. If more than one person is editing the same policy at the same time, the version saved last is the only version that will be stored.

To edit a policy:

1. In the table at the top of the Policies page, click the **Edit** hyperlink in the same row as the policy you want to edit.

The Update settings appear below the table. Make the necessary changes.

2. Select a policy file to associate with the policy using one of the following methods.
   - Upload a policy file – Type the name or Browse to transfer a copy of a file from the console application to the server application. If the SIF file is encrypted, type a password in the Password box to decrypt it.
   - Download this file from the Policy File Library – Transfer a copy of a policy file from the Policy File Library to the requesting computer by means of a modem or network. Click the **Choose** button to display a list of the policy files available in the library. Click a policy file to select it.

This option is available only if the server can access a Policy File Library.

3. Some policy files display a Policy Configuration box when you select them. If the Policy Configuration box appears, select the configuration settings in the box.
4. Change the name or optional description of the policy.
5. If you want the policy to be available to use in audits, check the **Make this policy active** box.

Clear the check box to make the policy unavailable to use in audits without deleting the policy.

6. Check the **Policy is kept up to date with Policy File Library** box if you want to regularly update the SIF files in this policy using the policy file library available on line.


This option is available only if the server can access a Policy File Library.

7. If you want the policy to be available to use in audits, check the **Make this policy active** box.

Clear the check box to make the policy unavailable to use in audits without deleting the policy.

8. If you want to policy to be available to use in self-service audits, check the **Available for use in self-service audits** box.

9. For Audit-On-Connect include the Link Type, Device Type, Posture Condition, Pass Results Valid For and Fail Results Valid For settings.

10. Set Windows Group Access. Enter Windows groups, separated by a comma, that can use this policy, remediate audit results generated using this policy, and view audit results for it. This establishes which users can access this policy and its audit results due to their role. If a Windows User Group isn't on the local computer, you'll need to enter the group in *domain*|*groupname* format.

- In the Use Policy field, enter the Windows groups who should be able to modify the policy.
- In the Remediate field, enter the Windows groups who should be able to remediate audit results generated using this policy.
- In the View Audit Results field, enter the Windows groups who should be able to view results from audits using the policy.

To grant all users access, type **Everyone**. To restrict all users, type **None**.

11. Click **Update** to revise the Policy settings in the database.

Any Audit-on-Connect or Audit-on-Schedule audits that are already based on this policy use the new policy settings the next time they run.

Deleting Policies

Click the **Delete** hyperlink for the policy that you want to remove. When you delete a policy, you remove it from the database. A warning appears to remind you that you are about to delete a record from the database. Cancel the action or delete the record.

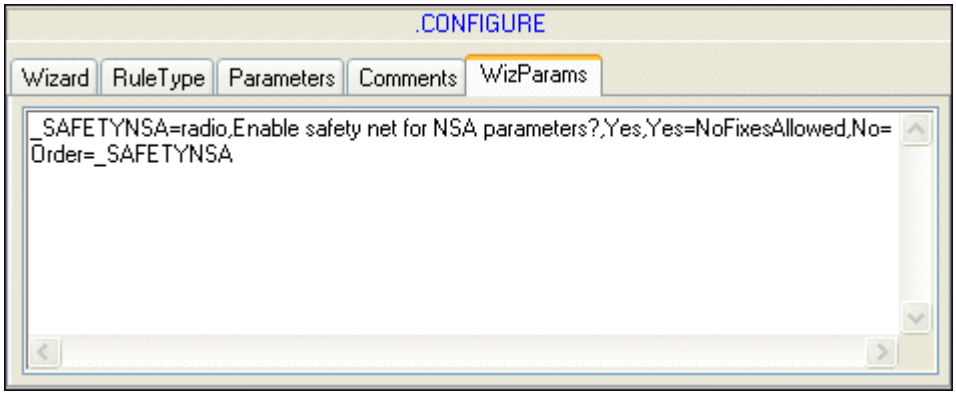
Configuring with Run-Time Policy Variables

Some policy files, such as the NSA Guidelines for Windows XP and Windows 2000, contain a special rule named .CONFIGURE. The .CONFIGURE rule allows you to configure your policy files and set global parameters for policy files at run time.

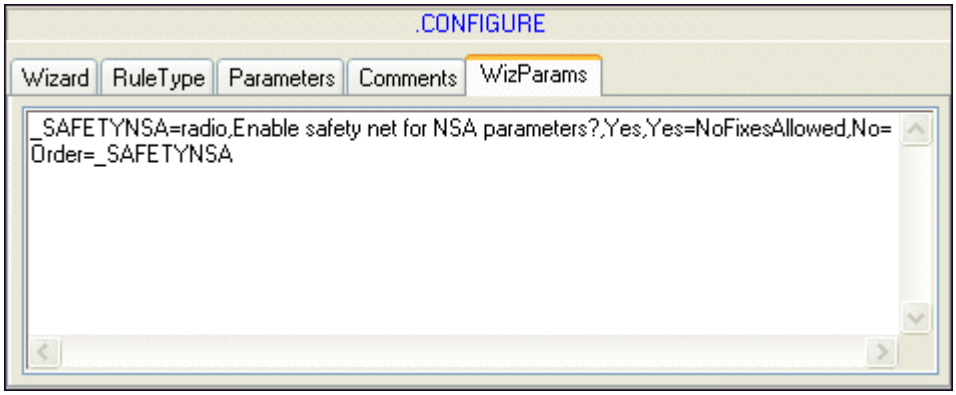
Certain information is unique and distinct between systems or groups of systems. A run-time policy variable allows administrators to use a single policy file but allows identification of unique rules that requires variable information. When a policy file uses a variable, your organization can use one policy file for multiple conditions where variables differ between departments or Machine Lists. For example, a variable might rename administrator accounts, change the members of an administrator account, or define the groups to which certain policies apply.

To understand the run-time policy variable, note the following settings in the NSA Guidelines for Windows XP and Windows 2000:

1. The name for the new rule must be .CONFIGURE.
2. The check type can be blank, or you can type CONFIGURE.
3. In the **Parameters** tab, the **Config** parameter is set to .CONFIGURE (Config=.CONFIGURE). When you set the Config key, the **WizParams** tab appears. On this tab you can type text using the WizParams syntax that controls the available text, input options, and parameters to modify in the **Wizard**.
4. View the **WizParams** tab to see the syntax that defines the Wizard's display for the rule. This example displays the question, "Enable safety net for NSA parameters?" In the **Wizard** you can select **Yes** or **No**.



The **Wizard** tab displays **MoreInfo** for this .CONFIGURE rule and the options defined in the Wizparams.



5. Review the **CrashOnAuditFull** rule in the **Parameters** tab. Note the **Modifiers** parameter, %get(.CONFIGURE:SAFETYNSA). The %get function calls the .CONFIGURE rule and uses the setting that enables the safety net setting for NSA parameters.

If you open the NSA Guidelines for Windows XP and Windows 2000 policy file, in the Preview pane you can click **Configure** to see the **Wizard** and the available options. If your policy file does not have a .CONFIGURE rule, the **Configure** link does not appear in the **Preview** pane.

Tip: This example describes how to use a .CONFIGURE rule in the console application. Rather than change the parameters there, you can select the variable settings in the server application

and modify the .CONFIGURE rule. When you create a new Policy and select an associated policy file, the server application determines if a .CONFIGURE rule exists and displays prompts for modifications. This rule may require synchronization between the database and the policy file. To synchronize the database and the new file, save the policy file in the database with a new name with new parameters for the .CONFIGURE rule, if previously saved in the database.

Scopes

Scopes

A scope is a set of target systems that get audited together when using Audit-on-Connect. Each scope is associated with one or more policies, which indicates how to audit the scope. When a system connects to the network, the server software checks all scopes to see if the system falls within one. If it does, and it is not part of an exception, it gets audited using the policy associated with the scope.

All scopes are assigned an order number. The first scope that matches the system is the scope used for the audit. All systems in the scope get audited.

The Scopes page displays the Scopes table and lets you add, edit, and delete scopes.

Add a New Scope

1. Click **Add New** on the Scopes page.
2. If you want to use an order number other than the one automatically generated, type one in the Order box.

   Order number is the numeric order in which the scope should be checked for resolution. SecurityExpressions Audit & Compliance Server automatically increments the order number. If you enter a new number or change the order, the application automatically rearranges the order of any existing scopes. For example, if you already have scopes 1 through 4 in the table and you create a new scope with an order number of 1, the existing scopes become scopes 2 through 5.

3. In the Name box, type a scope name.
4. Select the scope type.

   You may define scopes of the following types:

   - IP Range
   - Windows Domain This scope only works if you are using the Active Directory connection monitor.
   - Org Unit
   - DNS Domain Name
   - Device Type
   - Machine List
   - Expression
   - Detection Method

5. Enter values to determine which target systems belong to the scope. The values entered are determined valid or invalid depending on the scope type selected.

All scope types except Expression can accept as many values as you want to enter, listing one value per line. Scope type Expression only accepts one expression.

6. Indicate if the network link speed of the systems in this scope are Unspecified, Slow or Fast.

If all systems in the scope use a fast connection, for example, indicating this in the scope's definition prevents the need to check each system's speed during audits. Select Unspecified if you are unsure of network-connection speed or the scope contains a mix of slow and fast connections.

7. Type the Username and Password (credentials) needed to access the scope.

You may use variables in the user name, such as %computer% and %computershortname%, to access all target systems in the scope more efficiently. These variables return the target system's name. The variable you want to use depends on how your organization's DNS server is configured. Use %computer% if DNS returns short names. Use %computershortname% if DNS returns fully qualified names. For example, if DNS returns "hostname.domain.com," %computershortname% would change it to "hostname."

In order for the variable to work, the password of the account you're using must be the same to access all systems in the scope.

If you use the Windows connection method to audit systems in a workgroup, or if you're logging on using a local Windows user account instead of a domain account, you must include the system names in the Username box in this format: *systemvariable**username*, where *systemvariable* is either %computer% or %computershortname%.

Credential Precedence: If your organization uses the console application and someone delegated one or more database machine lists to the server application, *and* if one of the systems identified in this scope is also listed in one of those database machine lists, the server uses the database machine list's credentials to access the system rather than the scope credentials you enter here.

8. Select one or more policies to use to audit the targets in this scope from the Policies list.

Only the policies to which you have Use access rights appear for selection. Access rights are set in the Windows Group Access options on the Policies page. If you can't find a policy you need to use, ask the policy's creator to add you to one of the Windows User Groups with access rights to the policy.

9. If you have Altiris Notification Server and you want to send information about the audits generated on this schedule to Notification Server, select **Send a Notification Server Event**. If you prefer to send this information after each target computer is audited, select **Send a Notification Server Event for each target**.

10. If you want to send one or more notifications when an audit based on this scope occurs, select them in the Notification Options section.

You may use notifications created in SecurityExpressions console in addition to the ones created in SecurityExpressions server. The Notification Options section lists notifications created in both applications.

There are five conditions under which you can send notifications. Check which notification(s) you want to send when each condition occurs.

Device Connect Notifications - Sends selected notifications when a device is detected in this Scope, regardless of audit posture. This value may be blank.

Pass Notifications - Sends selected notifications if the audit's group posture result is Pass.

Fail Notifications - Sends selected notifications if the audit's group posture result is Fail.

Error Notifications - Sends selected notifications if the audit's group posture result is Error.

Connection Error Notifications - Sends selected notifications if the audit cannot connect to at least one target system.

SE Console Notifications - Lets you select notifications configured in the console application, if any exist. Select as many as you want.

11. Set Windows Group Access. Enter Windows groups, separated by a comma, that can view audit results for this scope. This establishes which users can access this scope's audit results due to their role. If a Windows User Group isn't on the local computer, you'll need to enter the group in *domain**groupname* format.

In the View Audit Results field, enter the Windows groups who should be able to view results from audits using the scope. To grant all users access, type **Everyone**. To restrict all users, type **None**.

If a computer is listed in multiple scopes, the only Windows Group Access settings that apply to the audit results are the ones from the scope used by the audit. Also, if a global machine list has Windows Group Results Access restricted in the ML Access page, the restrictions do not affect viewing audit results when a scope is a machine list scope. Only the Windows Group Results Access setting for the scope applies.

12. Click **Add** to store the new Scope in the database.

Edit a Scope

1. Click the **Edit** hyperlink on the Scopes table to select the row to edit.
2. Make any necessary modifications to:
   - order number

   Note: If you change the order, the application automatically rearranges the order of any existing scopes. For example, if you already have scopes 1 through 4 in the table and you create a new scope with an order number of 1, the existing scopes become scopes 2 through 5.

   - scope name
   - scope type
   - values for the scope type
   - link speed
   - user name (variables allowed)
   - password
   - policies

- notifications
- Windows Group access

Credential Precedence: If your organization uses the console application and someone delegated one or more database machine lists to the server application, *and* if one of the systems identified in this scope is also listed in one of those database machine lists, the server uses the database machine list's credentials to access the system rather than the scope credentials you enter here.

3. Click **Update** to store the new Scope configuration in the database.

Scopes Table

The Scopes table identifies each scope. The columns include:

Column	Description
Edit	Make changes to this policy entry in the table.
Delete	Remove this entry from the table.
Order	Numeric order in which the scopes should be checked when a computer connects to the network.
Name	Name of the scope.
Type	You may define scopes of the following types: IP Range Windows Domain This scope only works if you are using the Active Directory connection monitor. Org Unit DNS Domain Name Device Type Machine List Expression Detection Method
Value	The values that determine which target systems belong to the scope. The values entered are determined valid or invalid depending on the scope type selected. All scope types except Expression can accept as many values as you want to enter, listing one value per line. Scope type Expression only accepts one expression.
Link Speed	Indicate whether the network-connection speed of the systems in this scope is Unspecified, Slow or Fast. If all systems in the scope use a fast connection, for example, indicating this in the scope's definition prevents the need to check each system's speed during audits. Select Unspecified if you are unsure of network-connection speed or the scope contains a mix of slow and fast connections.
Username	User name of the credentials to use when auditing computers in this scope.
Policies	Names of the policies to use when auditing computers in this scope.
Device Connect Notifications	Notifications to run when a computer in this scope is detected, regardless of audit posture. This value may be

	blank.
Pass Notifications	Notifications to run when the Group Posture of an audit in this scope is PASS. This value may be blank.
Fail Notifications	Notifications to run when the Group Posture of an audit in this Scope is FAIL. This value may be blank.
Error Notifications	Notifications to run when the Group Posture of an audit in this Scope is ERROR. This value may be blank.
Connection Error Notifications	Notifications to run when the Group Posture of an audit in this Scope is CONN_ERROR. This value may be blank.
SE Console Notifications	Notifications from the console application to run when a computer in this scope is detected. This value may be blank.
Windows Group Results Access	Specify the Windows User Groups who can access results from audits that used this scope, if you want to restrict access to this scope's audit results. Displays "Everyone" if the scope's audit results aren't restricted.

Deleting Scopes

To delete a scope, click the **Delete** hyperlink for the scope in the table. When you delete a scope, you remove it from the database. A warning appears to remind you that you are about to delete a record from the database. At this time, you can cancel the action or delete the record.

DNS Domain Name Scopes

A domain written in DNS format. You may use the * wild card to represent a range of system names, as in "*.symantec.com".

A system matches this scope if its fully qualified domain name matches the value entered. You can also use any valid shell expression to match against a target's fully qualified domain name. If the server does not know the fully qualified name (typically from a reverse DNS lookup), then it attempts to match the target's IP address against the shell expression.

Expression Scopes

You may use an expression to combine more than one scope type into one unified scope of target systems. Use functions, Boolean operators and parentheses to construct your expression. Function names are not case sensitive. You may use more than one line to enter an expression.

Unlike the other scopes, expression scopes can only accept one entry. Regardless of how many lines long a scope is, all lines are treated as a single expression.

Example: (IPRANGE(12.2.1.0/24) || IPRANGE(11.2.1.0/20)) && !DOMAIN(symantec.com)

Supported Operators

Operator	Description
&&	Logical AND
||	Logical OR
!	Logical NOT

Supported Functions

Function	Argument	Description
iprange	a valid IP range	Returns TRUE if the target computer is a member of the IP range.
domain	a windows domain in Netbios or DNS format	Returns TRUE if the target computer is a member of the windows domain.
machinelist	a database machine list created using the console application	Returns TRUE if the target is a member of the machine list.
devicetype	a valid device type	Returns TRUE if the target is the type of device specified.
fqdnmatch	a shell expression	Returns TRUE if the target's full qualified domain name matches the shell expression.
ou	the name of an OU in Microsoft shorthand, and optionally an LDAP URL specifying what directory and credentials should be queried	Returns TRUE if the target is a member of the organizational unit.
detectionmethod	a method for detecting systems on the network	Returns TRUE if the target was detected on the network using this method.
aocserver	a shell expression	Returns TRUE if the server processing the connection event matches the shell expression.

Org Unit Scopes

Also known as an OU, a system's organizational unit is listed in the domain controller. The software searches OUs in order to find Active-Directory computer accounts. OU searches begin at the directory's default naming context.

Use Microsoft shorthand notation to type OUs. You do not need to type OUs in a case-sensitive manner. For example, the Active Directory DN of "ou=A,ou=B,dc=symantec,dc=com" would be entered as "B/A." If your computer accounts are located in Active Directory's default location of "cn=computers,dc=symantec,dc=com," you can simply enter "computers" to search for all computer accounts.


If you're running the server application on a system that's not a member of an Active Directory domain, you'll need to override the directory, protocol and login credentials to the directory by specifying an LDAP URL as the first OU. The syntax is "ldap://[user:password@]host[:port]." The User can be in Microsoft format such as "user@domain.com" or in standard LDAP format such as "cn=user,dc=symantec,dc=com."

A system matches this scope if its Active-Directory computer account matches the value entered.

Detection Method Scopes

Audits can detect systems on the network using the following methods: DHCP, EVENTLOG, NAC, self-service (for self-service audits).

A system matches this scope if the connection monitor used to connect to it matches the value entered.

Device Type Scopes

Lets you indicate a kind of system to audit. Choices are Windows, UNIX, or Unknown.

A system matches this scope if it's the kind of system selected. Selecting Unknown includes all systems.

IP Range Scopes

A system matches this scope if its IP address is in the range. Use **-** or **:** to indicate an IP range.

Ex.:192.168.10.1-62

Use **/** to indicate an IP range expressed using netmask length.

Ex.: 10.0.3.0/24

You can also enter single IP addresses.

Machine List Scopes

If your organization uses the console application and someone created one or more database machine lists (also known as global machine lists) on it, you may use this scope. Type the names of database machine lists from the console.

A system matches this scope if it's in the machine list.

If a global machine list has Windows Group Results Access restricted in the ML Access page, the restrictions do not affect viewing audit results when a scope is a machine list scope. Only the Windows Group Results Access setting for the scope applies.

Windows Domain Scopes

A system matches this scope if its fully qualified domain name matches the value entered. Type domains in either Netbios (SYMANTEC) or DNS (symantec.com) format.

This scope only works if you are using the Active Directory connection monitor.

Notifications

Notifications

You can opt to receive email or program-output notifications when audits occur. Notifications apply to Audit-On-Schedule or Audit-On-Connect results and each audit can have one or more notification actions upon completion.

You may use notifications created in SecurityExpressions console in addition to the ones created in SecurityExpressions server. This application lets you select notifications created in both applications in the Schedules Tasks page and the Scopes page.

The Notifications table displays the notification Name, Type, and Values. From this page you create an email or command notification that you can edit or delete.

Creating New Command Notifications

To create a new command notification:

1. Click **Add New**.
2. Provide a **Notification Name**, a customized name of the notification to appear in the table.
3. Select Command as the **Type**.
4. Type the Command to run, which may be a URL. Include the command Arguments. You can pass variables to the command.

   If the command is a program, programs expect dependent files to be in the \system32\ folder.

5. Click **Add New**.

Creating New Email Notifications

When you create an email notification, you must identify the SMTP email server and the address from which the email should be sent.

To create a new email notification:

1. Click **Add New**.
2. Provide a Notification Name, a customized name of the notification to appear in the table.
3. Select Email as the Type.
4. Complete the following email information:

   To – person receiving the notification. This address appears as the Value in the table. Or Select allows you to select a previously entered email address.

   Subject – Notification topic. Or Select allows you to select a previously entered subject.

   Message – Text of the email notification, including variables.

   Examples: An audit has finished: %COMPUTER%

   The group posture result is %GROUPPOSTURERESULT%.

   Click here for the report: %RESULTLINK%

5. Select **Attach trace route information for Audit-on-Connect** for the message body to include the trace route. The message body always includes a link to the report for the audit that caused this notification.
6. **Recommended:** Click **Send Test** to make sure the notification will send as configured.
7. Click **Add New.**

Set Server for Email Notifications

Email notifications require that you set the SMTP server settings. These global settings include the email server (the name of the server through which to send email notifications) and the sender address (the email address of the person sending the email notifications).

Editing Notifications

To edit a Notification, click the Edit hyperlink on the Notifications table to select the row to edit. Make the necessary modifications and click **Update**.

To Edit an email notification, make the necessary modifications to:

- Notification Name
- To – person receiving the notification. This address appears as the Value in the table.
- Subject – Notification topic
- Message – Text of the email notification, including variables.
    - Check or clear the **Attach trace route information for Audit-on-Connect** box to determine whether or not the message body will include the trace route.

 We recommend you click **Send Test** to make sure the modified notification will send.

To Edit a command notification, make the necessary modifications to:

- Notification Name
- Command
- Optional Arguments

Deleting Notifications

Creating New Email Notifications

To create a new email notification:

1. Click **Add New**.
2. Provide a Notification Name, a customized name of the notification to appear in the table.
3. Select Email as the Type.
4. Complete the following email information:

   To – person receiving the notification. This address appears as the Value in the table. Or Select allows you to select a previously entered email address.

   Subject – Notification topic. Or Select allows you to select a previously entered subject.

   Message – Text of the email notification, including variables.

   Examples: An audit has finished: %COMPUTER%

   The group posture result is %GROUPPOSTURERESULT%.

   Click here for the report: %RESULTLINK%

5. Select **Attach trace route information for Audit-on-Connect** for the message body to include the trace route. The message body always includes a link to the report for the audit that caused this notification.
6. **Recommended:** Click **Send Test** to make sure the notification will send as configured.
7. Click **Add New.**

Creating New Command Notifications

To create a new command notification:

1. Click **Add New** in the Notifications page.
2. Provide a Notification Name, a customized name of the notification to appear in the table.
3. Select **Command** as the Type.
4. Type the Command to run, which may be a URL. Include the command Arguments. You can pass variables to the command.

   If the command is a program, programs expect dependent files to be in the \system32\ folder.

5. Click **Add New**.

Deleting Notifications

Click the **Delete** hyperlink for the notification that you want to remove. When you delete a notification, you remove it from the database. A warning appears to remind you that you are about to delete a record from the database. At this time, you can cancel the action or delete the record.

Notification Variables

You can include the variables listed here in any text-entry setting in a notification.

%RESULTLINK% - URL of the results or report

%POLICY% - policy used to perform the audit

%DESCRIPTION% - description of the task that executed the audit, from the Description box located in the Task Options and Scheduling dialog box's List tab

To learn more about the Task Options and Scheduling dialog box, check the SecurityExpressions Console help.

%DATE% - the date this task ran

The following three variables will only return a value if statistics are available:

%COUNTPROBLEMS% - number of errors encountered during the audit

%COUNTRULES% - number of rules used to audit the machine list

%SCORE% - the overall score resulting from the audit

The following four variables will only return a value if the task only audited one system:

%IP% - IP address or name of the system being audited, depending which represents the system in the machine list

%COMPUTER% - identical to the %IP% variable

%HOST% - identical to the %IP% variable

%GROUPPOSTURERESULT% - posture result of the system being audited

Example

A Subject or Message may contain text such as "Latest SecurityExpressions audit located at %RESULTLINK%."

Exceptions

Exceptions

Exceptions prevent certain systems from ever getting audited, even if they fall within a scope. When a system connects to the network, the server software checks all scopes to see if the system falls within one. If it does, the server software then checks all exceptions to see if the system is listed in an exception. If it is, the system does not get audited.

To exclude the devices from an audit, you must add them to the Exceptions list through the Exceptions table. From the table you can Add, Edit or Delete the Exception.

Exceptions Table

Column	Description
Type	Type of device specification. May be a MAC address, a fully-qualified domain name, an IP address, or range of IP addresses.
Value	The value of Type. You may use the * wild card. You may also enter IP addresses and IP ranges if you selected **Fully Qualified Domain Name** as the type.
Expiration Date	Date when audits stop applying this exception. If Never, this exception does not expire.
Posture	Result returned when this device connects to the network.
Description	Exception or device description.

Adding Exceptions

To add new Exceptions:

1. Click **Add New** on the Exceptions page.
2. Select MAC address, Fully-Qualified Domain Name, or IP Address or Range as the **Type**.
3. Enter the **Value**.

   A MAC address that includes a wild card would be 00-08-74-35-**-** (you can use either **-** or **:** to parse a MAC address). A fully-qualified domain name that includes a wild card would be *.ids.symantec.com. If entering a range of IP addresses, use a hyphen between the lowest address and the highest address.

4. Select the Expiration Date from the calendar. This date indicates when audits stop applying this exception. If you want the Exception enforced indefinitely, select the **Never** check box.
5. Identify the **Group Posture** , such as Pass or Out of Scope, to return when the device connects to the network.
6. Optionally, type a short **Description** describing the exception or device.
7. Click **Add**.

Editing Exceptions

To edit Exceptions:

1. Click the Edit hyperlink on the Exceptions table to select the row to edit.
2. Modify the Exception parameters (**Type**, **Value**, **Expiration Date**, **Group Posture Result**)
3. Click **Update**.

Deleting Exceptions

To delete an Exception:

1. Click the **Edit** hyperlink on the Exceptions table to select the row to remove.
2. When you delete an Exception, you remove it from the database. A warning appears to remind you that you are about to delete a record from the database. Cancel the action or delete the record.

Connection Monitors

Connection Monitors

Connection Monitors are services that are installed on DHCP Servers, Active Directory Servers, or other servers that coordinate Audit-on-Connect sequences. They determine when a device connects to the network and then send a request to a server to perform an audit on that device. Each Connection Monitor uses a configuration file (dmconfig.txt) to store a list of audit servers to contact. This list includes a particular range of IP addresses, along with a distribution method to balance the load among the audit servers.

Most of the configuration work is in editing the configuration file (dmconfig.txt). The settings described here are only part of the process.

The SecurityExpressions Audit & Compliance Sever includes three types of Connection Monitors:

- DHCP Network Connection Monitor with access to network traffic, installed on any server, monitors network packets for those containing DHCP protocols.
- Microsoft DHCP Server Plug-In Connection Monitor, installed on the device running Windows DHCP server.
- Active Directory Connection Monitor, installed on any server on the domain, monitors Active Directory activity for when a new device appears on the network.

IP Address or Fully Qualified Name

List the IP address or fully-qualified name of the computer hosting a Connection Monitor.

You must configure the SecurityExpressions Audit & Compliance Sever with a list of the known Connection Monitors that will be listened to. If the IP address or the fully-qualified name of the Connection Monitor does not appear in the Device Connection Monitor list, the module is not listened to.

Add or remove the name of a new computer that hosts a Connection Monitor.

Specify Password and Encrypted Password

Specify and confirm a password. SecurityExpressions Audit & Compliance Server generates an encrypted password that you must add the to the configuration files for each of the Connection Monitors. Include the encrypted password in the [Options] section of the configuration file with the Password option.

Settings for DHCP Plug-In or DHCP Network Monitor Connection Monitors

When a connection event is detected by either of the DHCP connection monitors, the system may not yet be booted fully to a state that allows an audit to occur. In order to ensure that a system is audited properly when detected by a DHCP connection monitor, you can configure the system here to retry any failed connections. These settings control how many seconds will pass between retries and the number of times a connection will be retried before attempting to audit the system.

Configuring Connection Monitors


Most of the configuration work is in editing the configuration file (dmconfig.txt). The settings described here are only part of the process.

List the IP address or fully-qualified name of the computer hosting a Connection Monitor.

To add a Connection Monitor device to the list, type the IP address or fully-qualified device name and click **Add New**.

To remove a device from the list, select the IP address or fully-qualified device name and click **Remove.**

Once you set the settings on this page, you must enable the connection monitor.

Enabling Connection Monitors

To fully enable a Connection Monitor, you must set complete computer and credential settings:

- IP address or fully-qualified computer name - To enable a Connection Monitor you must add the IP address or fully-qualified computer name of the devices with installed Connection Monitors.
- Password and encrypted password - When you create and verify a password, an encrypted password appears. You must add the encrypted password for each monitor to the configuration file named dmconfig.txt, which resides in the same directory as the Connection Monitor.
- Settings for DHCP Plug-In or DHCP Network Connection Monitors - When a connection event is detected by either of the DHCP connection monitors, the system may not yet be booted fully to a state that allows an audit to occur. In order to ensure that a system is audited properly when detected by a DHCP connection monitor, you can configure the system here to retry any failed connections. These settings control how many seconds will pass between retries and the number of times a connection will be retried before attempting to audit the system.

Include the encrypted password in the Options section of the configuration file. For example,

[Options]

Port = 9009

Password = AES: cb789817f8d99c7e5a1e5beb8510bf71

Once you enable the connection monitor, it can be processed at any time.

Connection Monitor Configuration File

Connection Monitors use a text file named dmconfig.txt that resides in the same directory as the Connection Monitor (\Program Files\Altiris\Security Management\SecurityExpressions Connection Monitors). The file contains four sections. You must complete the IP Range and Options sections. The Default and Active Directory sections are optional.

Tip: If you are using more than one connection monitor on the same computer, use the same configuration file to configure them.

After editing and saving the configuration file, you must stop and restart the DHCP or Active Directory monitor service through the Service Management Console, which is accessible through Administrative Tools.

Tip: Use the **#** character at the beginning of all comment lines to ensure they get ignored when the file processes.

Click here to review the configuration file's syntax.

IP Range Section

Create one section per IP range. The IP range section consists of:

IP and default IP range of the target devices

Distribution methods

Comma-separated list of audit server names

IP Ranges

The IP Ranges section of the configuration file identifies the IP ranges of the device groups.

- Zero or more IP ranges – IP ranges divide newly detected devices into different groups. If an IP range does not exist, no devices are audited.
- Default IP range – All IP addresses not previously placed in one of the IP range groups.

Distribution Methods

Two distribution methods, Round Robin and First Available, comprise the Connection Monitor sequencing. To indicate which method you want to use, type either **Round Robin** or **First Available**.

Round Robin – Each SecurityExpressions Audit & Compliance Server in the list is contacted in sequence as new devices are detected, wrapping around to the beginning of the list after contacting every listed audit server. If a connection times out, the Connection Monitor tries the next audit server in the list until it attempts contact with every audit server on the list.

First Available – To begin, the Connection Monitor always contacts the first Audit & Compliance Server. If the connection fails, it tries to contact the second audit server, and so forth, until connection is successful after trying to contact one or every audit server on the list. The First Available method is important if the first server goes down.

Comma-Separated List of Servers

Includes the names of the audit servers. A comma separates each server name.

Options

The Options section of the configuration file contains any settings needed to control the Connection Monitors, such as enabling logging and identifying the location and name of the log file.

Port

The port you want a connection monitor to use to communicate with the server software. This entry must match the server's configuration, which is 9009.

LogEnable

Typing **True** turns logging on. Typing **False** turns logging off.

LogFile

Identifies the log file location and file name.

Password

Add the encrypted password.

DropPXE

Enables you to ignore PXE DHCP requests if using the DHCP Network Connection Monitor or Microsoft DHCP Server Connection Monitor. When the PXE gets a DHCP request, Audit-on-Connect is triggered. When PXE is done and Windows restarts, Audit-on-Connect is triggered once more, not necessarily using the same IP address.

If set to 1, PXE DHCP packets are ignored. If set to 0, they are processed.

Default

The Default section identifies all IP addresses not previously placed in one of the IP range groups.

IPRange

Set to default.

AuditServers

Comma-separated name of the servers.

DistributionMethod

Set to Round Robin or First Available.

Active Directory (Active Directory Connection Monitor only)

Set the Active Directory (event log) monitoring options.

IncludeAllDomainControllers

Retrieves names of all Domain Controllers on the Domain system where the monitor resides and monitors the event logs of all Domain Controllers. One (1) is the default setting. If IncludeAllDomainControllers=0 you must add the Include key and identify the device to monitor.

Exclude

Comma-separated list of device names to omit from monitoring.

Include

Comma-separated list of device names to monitor.

Processing the Configuration File

When the Connection Monitor recognizes a new device on the network, it compares the device IP address to the IP ranges defined in the configuration file, excluding the Default settings, starting with the first range in the file and proceeding in order. If the address falls in one of the IP ranges, that group's audit server list and distribution method determine where to connect.

If the IP address does not fall within any of the specified ranges, a group whose IPRange=Default accesses the audit server list and distribution method.

You do not have to specify a Default IP range. However, if a Default range does not exist and the IP address does not correspond to any of the defined ranges, the monitor does not contact the audit server and the device remains unaudited.

Configuration File Syntax

To specify configuration data, you manually edit the dmconfig.txt file and include the required information about the IP ranges. After editing the configuration file, you must stop and restart the service through the Service Management Console, which is accessible through Administrative Tools.

Tip: If you are using more than one connection monitor on the same computer, use the same configuration file to configure them.


Be aware that if you're using the DHCP Plug-In Connection Monitor, it's Microsoft's DHCP Server Service that you have to stop. Since this service controls other functions on the network, stopping it might have other temporary effects on the network.

Tip: Use the **#** character at the beginning of all comment lines to ensure they get ignored when the file processes.

The configuration file syntax is similar to .ini file syntax, such as:

[IP_RANGE_1]

IPRange=10.0.3.0:254

AuditServers=server1,server2

DistributionMethod=Round Robin

Comment=Home office ip addresses

[IP_RANGE_2]

IPRange=10.0.2.0:254

AuditServers=server3,server1,server2

DistributionMethod=First Available

Comment=California office ip's

[Default]

IPRange=Default

AuditServers=server1,server2

DistributionMethod=Round Robin

Comment=Catch anything not explicitly specified

[Options]

Port = 9009

Password = AES: cb789817f8d99c7e5a1e5beb8510bf71

LogEnable=True

LogFile=c:\temp\dhcpdetect.log

DropPXE=1

[ActiveDirectory]

IncludeAllDomainControllers=1

Exclude=server1, server2

Include=server3

Network

Slow Links

Enable slow link detection tests the connection to a computer to see if it is through a 56 KB modem or a similarly slow device. If the server software detects a slow link, it skips auditing with any policies set only for fast links.

Enabling slow link detection might extend processing time.

Trace Route Information

Trace route is a TCP/IP utility that allows the user to determine the route that packets are taking to a particular host. Your notifications can include a trace route if you select this optional setting, **Make trace route information available to notifications**. Determining trace route information may be slow.

Network Admissions Control

The Network Admissions Control section of the Network page enables Cisco Network Admissions Control (NAC) to work with the server software. NAC allows network access only to trusted end-point devices that can verify their compliance to network security policies. It can permit, deny or restrict network access to any device as well as quarantine and remediate non-compliant devices.

The server software communicates with NAC through Cisco Secure Access Control Server (ACS). ACS uses the server software as its External Posture Validation Audit Server. External Posture Validation Audit Server sends *posture tokens* to ACS that indicate the audit status of systems. Using that information, NAC can determine whether or not these systems are in compliance.

The server software frequently checks target systems to keep the posture tokens updated. The possible posture tokens are:

- **Healthy -** The system had a posture result of Pass when checked.
- **Quarantined -** The system had a posture result of Fail when checked.
- **Transition -** The system was in the middle of an audit when checked.
- **Unknown -** The server software does not recognize the system, cannot connect to the system or lost connectivity during the last audit.

To configure the server software to work with NAC, select settings in the following categories.

Unmanaged Systems

An unmanaged system is a system on the network that the server software does not recognize or cannot connect to.

Initial Token

Sends the posture token you select to ACS if the server cannot connect to a system.

Token After Self Audit

Sends the posture token you select to ACS if a quarantined system fails a self-service audit.

Cache Validity Duration

Select how long a posture token of Healthy should remain valid. This is a way to control how often the server software verifies that an unmanaged system is still in compliance with network security policies after it receives a Healthy posture token. If you select **Forever**, the system's Healthy token will never expire.

Managed Systems

A managed system is a system on the network that the server software can connect to and audit using the appropriate credentials. It is a target system or potential target system.

Initial Token

Sends the posture token you select to ACS if a system receives a posture result of Fail.

Both Managed and Unmanaged

Network Access Device (NAD) Polling

Select how often ACS should poll the server software for the latest status of target systems. If it finds any updated policies:
- the server audits managed target systems with a valid Healthy token unless the policy cache settings indicate otherwise.
- NAC places Healthy unmanaged systems into quarantine as soon as their Cache Validity Duration expires.

Healthy

Select how often ACS should poll the server software for the latest status of target systems when the managed target systems have a valid Healthy token. In addition to selecting specific time intervals, you can opt to poll healthy systems as often as the smallest time interval entered in the Cache Pass For option, found in the Policies table, for all policies in the scope used.

Quarantined/Unknown

Select how often ACS should poll the server software for the latest status of target systems when the managed target systems have a valid Quarantined or Unknown token.


Make sure you set the Cache Fail For option, found in the Policies table, for a length of time longer than the time you select here. If you do not set these times strategically, systems might not be able to get out of quarantine.

Reaudit if quarantined

Check this box if you want to reaudit systems with a valid Quarantined or Unknown token. Quarantined and unknown systems will get audited at the frequency you selected in the Quarantined/Unknown drop-down list until they receive a Healthy token.


As you're selecting the settings on this page, keep in mind NAC's Audit in Progress Poll Hint Timeout. The poll-timeout hint is a length of time the server software passes to ACS that indicates the next time it would be appropriate to request another token. NAC uses this value to reduce the number of communication round trips between the servers. The settings affect the poll-timeout hint in the following ways:

- If a system has a **Healthy token**, the poll-timeout hint returned is the length of time selected from the Healthy drop-down list.
- If a system has a **Quarantined or Unknown token**, the timeout hint returned is the length of time selected from the Quarantined/Unknown drop-down list.

If a system does not have a valid Healthy, Quarantined or Unknown token when sent to the auditing queue, the server software returns a timeout hint that takes into account the number of hosts currently waiting to be audited and the average time to complete an audit.

Redirection Web Page

A read-only line that reminds you to configure ACS so that NAD redirects users who try to connect to the network from quarantined systems to the URL listed.

Redirection Web Page Behavior

Select the information and resources the redirection Web page should provide to users on quarantined systems if URL redirection is configured in ACS. The options are:

- **Display a message that the user must contact an administrator for access and leave in quarantine.** To customize this message, modify NAC/NotHealthy.aspx.
- **Display the results of the failed audit and a message stating that an administrator has been notified, then grant access to the network and remove from quarantine.**
  Managed Systems - NAC removes the system from quarantine by sending a token of Healthy to ACS. To customize the message for managed systems, modify NAC/PermitAccess.aspx.

  Unmanaged Systems - The Web page displays instructions on how to perform a self audit. When users click **Next**, NAC removes the system from quarantine by sending a token of Healthy to ACS. To customize the message for unmanaged systems, modify NAC/UnmanagedSelfAudit.aspx.
- **Provide help with remediation. Display the following URL containing instructions for self-remediation. Allow the user to perform self-service audits to verify.** Type a URL where users can get remediation instructions. After they remediate, the redirection Web page describes how to perform a self audit. To customize this message, modify NAC/SelfRemediate.aspx.

Audit on Connect Tracing

Audit on Connect Tracing

Audit on Connect audit events are complex, involving lots of variables. If you suspect Audit on Connect is not operating as expected, you would have a hard time troubleshooting the problem on your own. The AOC Tracing page keeps track of any Audit on Connect activity occurring during a set time period, recording the details of the activity caused by the audit event and listing the Audit on Connect settings configured for the audit event. This empowers you to troubleshoot possible problems in Audit on Connect activity or configuration.

AOC tracing shows:

- when a computer listed in a scope connects to the network
- which device type, policies, scope, notifications, exceptions, and connection-monitor type were involved in the audit event
- if a slow link was detected
- trace-route information, if enabled
- Cisco Network Admissions Control (NAC) activity, if any
- if a cached policy file is used

Tip: AOC tracing is designed to be turned on and off, running for set lengths of time. It does not record constantly or permanently log tracing data. If you suspect problems, determine when the suspect activity will occur. Then turn it on and set it to run for the length of time you expect the activity to take.

To trace Audit on Connect activity:

1. Determine when the suspect activity will start and how long it will take to finish.
2. When the suspect activity is about to begin, type the hours and minutes you expect the activity to take in the Run AOC Trace for fields and click **Start Trace**.


If you type 0 hours and 0 minutes, the trace will not occur.

3. Click **Refresh** any time you want to check on the activity that's occurred so far. This displays the latest trace data on the page.


Trace data does not automatically display when AOC tracing is on. You need to click **Refresh** whenever you want to see the latest trace data.

While AOC tracing is on, it captures whether or not any activity occurs. If no trace data appears, then no activity occurred. This could mean:

- you miscalculated when you should turn on AOC tracing to capture the activity you're looking for
- your suspicions are true: something is wrong with Audit on Connect and it's not running when expected

The trace data from the last time you refreshed remains on the page until you click **Delete Trace Data**.

Audit-On-Schedule

What is Audit-on-Schedule?

Audit-on-Schedule is an auditing method that audits a group of systems at scheduled intervals. You create a scheduled task that audits all systems in a machine list based on a policy. When the audit is finished, the task can send notifications indicating the audit is done and where to view audit results.

Use the following pages to configure Audit-on-Schedule:

Policies

Notifications

My Machine Lists

Scheduled Tasks

First create policies, notifications and machine lists to add to scheduled audit tasks. Then create a task. Once the task is scheduled, it runs automatically

Policies

Policies Page

When you create a new policy, you assign a name and a policy file (.sif) to the policy. Note that policies differ from policy files: a *policy* contains a designated *policy file*.

From the Policies page you create policies to define the audits. You also edit or delete existing policies. If performing an Audit-on-Connect audit, you also set the run-time variables on the Policies page.


Policies are saved to the database. If more than one person is editing the same policy at the same time, the version saved last is the only version that will be stored.

Note that you can associate one or more policy files with specific conditions and the scope.

The Policies table displays available policies for the audits and policy configurations.

Policies Table

The Policies table displays available policies for the audits and policy configurations. The Policies table consists of the following columns:

Column	Description
Active	If Yes, then apply the policy. If the policy is active, within that Scope, the policy will be applied. If No, the policy is not applied but will not be deleted.
Edit	Make changes to this policy entry in the table.
Delete	Remove this entry from the table.
Name	Policy name as it is listed for selection when creating a scope or scheduled task.

Description	Optional statement about the policy.
Policy File	Name of the policy file (.sif), from the policy file library or a customized policy file.
Last Updated	Date and time the policy file was last saved to the database.
Configure	Some policy files, such as the NSA Guidelines for Windows XP and Windows 2000, contain a special rule named .CONFIGURE. The .CONFIGURE rule allows you to configure your policy files and set global parameters for policy files at run time. This column shows whether or not the policy file contains the .CONFIGURE rule. Certain information is unique and distinct between systems or groups of systems. A run-time policy variable allows administrators to use a single policy file but allows identification of unique rules that require variable information.
Windows Group Use Access	Specify the Windows User Groups who can use this policy, if you want to restrict access to this policy. Displays "Everyone" if the policy isn't restricted.
Windows Group Remediation Access	Specify the Windows User Groups who can remediate audit results generated using this policy, if you want to restrict access to remediation through this policy. Displays "Everyone" if remediation through this policy isn't restricted.
Windows Group Results Access	Specify the Windows User Groups who can access results from audits that used this policy, if you want to restrict access to this policy's audit results. Displays "Everyone" if the policy's audit results aren't restricted.
Use on Link Type (Audit-On-Connect only)	Specify whether to run this policy over fast or slow connections, or both kinds. Some policies might not be appropriate to run over slow connections if they request a large amount of data. For example, applying large policy files like MS Fixes over a slow network connection, such as a 56K modem, can take a long time.
Device Types (Audit-On-Connect only)	Audit with this policy on these device types. Choices include Windows, UNIX, and Unknown.
Posture Condition (Fail If) (Audit-On-Connect only)	The rules for determining if the resulting posture after auditing with this policy is Pass or Fail. The posture is based on all policy-file rule results (OK, Not OK), plus impact and priority settings. Available posture conditions are: • Always Pass • Any Fail • Any Not OK • Any Not OK with Priority • Any Not OK with Score • Any Not OK with Impact • Any Not OK with Key
Cache Pass For (Audit-On-Connect Only)	Specify how long posture results remain valid when the system passes an audit based on this policy. This is a way to control how often a system gets audited — as long as a

	posture result remains valid, the software won't attempt to audit a system if it connects to the network again. Instead, it returns a posture result of Pass.
Cache Fail For (Audit-On-Connect Only)	Specify how long posture results remain valid when the system fails an audit based on this policy. This is a way to control how often a system gets audited — as long as a posture result remains valid, the software won't attempt to audit a system if it connects to the network again. Instead, it returns a posture result of Fail.

Adding Policies

To create a policy:

1. Click **Add New** on the Policies page.
2. Select a policy file to associate with the policy using one of the following methods.
    - Upload a policy file – Type the name or Browse for a SIF file. If the SIF file is encrypted, type a password in the Password box to decrypt it.
    - Download this file from the Policy File Library – Transfers a copy of a policy file from the Policy File Library over the network. Click the **Choose** button to display a list of the policy files available in the library. Click a policy file to select it.

    This option is available only if the server can access a Policy File Library.
3. Optional: In the Name box, change the name of the policy.

    The name of the policy file you selected in step 2 appeared in this box when you selected it.
4. Optional: In the Description box, type a description of the policy.
5. If you uploaded a policy file that's encrypted, type a password to decrypt it in the Password box.

    Policy files downloaded from the Policy File Library aren't encrypted.
6. If you want the policy to be available to use in audits, check the **Make this policy active** box.

    Clear the check box to make the policy unavailable to use in audits without deleting the policy.
7. Check the **Policy is kept up to date with Policy File Library** box if you want to regularly update the SIF files in this policy using the policy file library available on line.

    This option is available only if the server can access a Policy File Library.
8. If you want the policy to be available to use in self-service audits, check the **Available for use in self-service audits** box.
9. Type a name and optional description of the policy.
10. For Audit-On-Connect include the Link Type, Device Type, Posture Condition, Pass Results Valid For and Fail Results Valid For settings.
11. Set Windows Group Access. Enter Windows groups, separated by a comma, that can use this policy, remediate audit results generated using this policy, and view audit results for this policy. This establishes which users can access this policy and its audit results due to their role. If

a Windows User Group isn't on the local computer, you'll need to enter the group in *domain**groupname* format.

- In the Use Policy field, enter the Windows groups who should be able to modify the policy.
- In the Remediate field, enter the Windows groups who should be able to remediate audit results generated using this policy.
- In the View Audit Results field, enter the Windows groups who should be able to view results from audits using the policy.

To grant all users access, type **Everyone**. To restrict all users, type **None**.

12. Click **Add Policy** to revise the policy settings in the database.

Some policy files display a Policy Configuration box at this point. If the Policy Configuration box appears, select the configuration settings in the box. Then click **Add Policy** again.

Now you may base audits on this policy when setting up Audit-on-Connect or Audit-on-Schedule.

Editing Policies

When editing a policy, you can modify any policy characteristics. For example, by clearing the **Make this policy active** check mark, that policy no longer applies for the Scope. You could also change the policy by selecting a previously saved file or uploading a policy file from our Web site.

Policies are saved to the database. If more than one person is editing the same policy at the same time, the version saved last is the only version that will be stored.

To edit a policy:

1. In the table at the top of the Policies page, click the **Edit** hyperlink in the same row as the policy you want to edit.

The Update settings appear below the table. Make the necessary changes.

2. Select a policy file to associate with the policy using one of the following methods.
   - Upload a policy file – Type the name or Browse to transfer a copy of a file from the console application to the server application. If the SIF file is encrypted, type a password in the Password box to decrypt it.
   - Download this file from the Policy File Library – Transfer a copy of a policy file from the Policy File Library to the requesting computer by means of a modem or network. Click the **Choose** button to display a list of the policy files available in the library. Click a policy file to select it.

   This option is available only if the server can access a Policy File Library.

3. Some policy files display a Policy Configuration box when you select them. If the Policy Configuration box appears, select the configuration settings in the box.

4. Change the name or optional description of the policy.

5. If you want the policy to be available to use in audits, check the **Make this policy active** box.

Clear the check box to make the policy unavailable to use in audits without deleting the policy.

6. Check the **Policy is kept up to date with Policy File Library** box if you want to regularly update the SIF files in this policy using the policy file library available on line.

This option is available only if the server can access a Policy File Library.

7. If you want the policy to be available to use in audits, check the **Make this policy active** box.

Clear the check box to make the policy unavailable to use in audits without deleting the policy.

8. If you want to policy to be available to use in self-service audits, check the **Available for use in self-service audits** box.

9. For Audit-On-Connect include the Link Type, Device Type, Posture Condition, Pass Results Valid For and Fail Results Valid For settings.

10. Set Windows Group Access. Enter Windows groups, separated by a comma, that can use this policy, remediate audit results generated using this policy, and view audit results for it. This establishes which users can access this policy and its audit results due to their role. If a Windows User Group isn't on the local computer, you'll need to enter the group in *domain**groupname* format.

- In the Use Policy field, enter the Windows groups who should be able to modify the policy.
- In the Remediate field, enter the Windows groups who should be able to remediate audit results generated using this policy.
- In the View Audit Results field, enter the Windows groups who should be able to view results from audits using the policy.

To grant all users access, type **Everyone**. To restrict all users, type **None**.

11. Click **Update** to revise the Policy settings in the database.

Any Audit-on-Connect or Audit-on-Schedule audits that are already based on this policy use the new policy settings the next time they run.

Deleting Policies

Click the **Delete** hyperlink for the policy that you want to remove. When you delete a policy, you remove it from the database. A warning appears to remind you that you are about to delete a record from the database. Cancel the action or delete the record.

Configuring with Run-Time Policy Variables

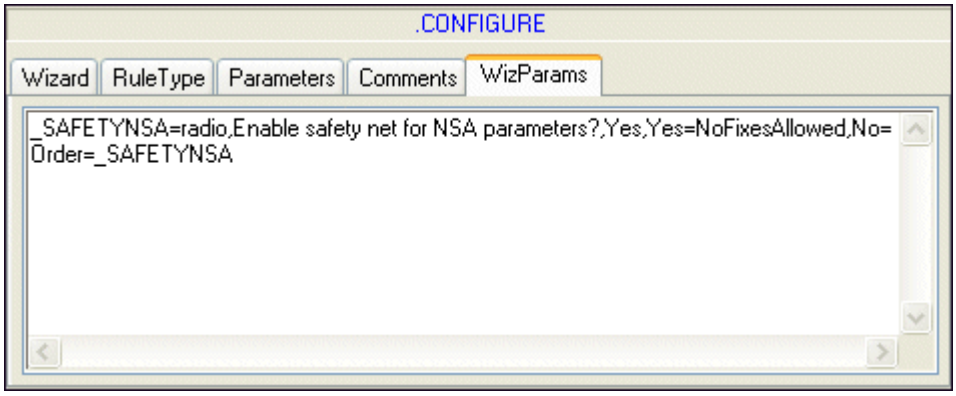
Some policy files, such as the NSA Guidelines for Windows XP and Windows 2000, contain a special rule named .CONFIGURE. The .CONFIGURE rule allows you to configure your policy files and set global parameters for policy files at run time.

Certain information is unique and distinct between systems or groups of systems. A run-time policy variable allows administrators to use a single policy file but allows identification of unique rules that requires variable information. When a policy file uses a variable, your organization can use one policy file for multiple conditions where variables differ between departments or Machine Lists. For example, a variable might rename administrator accounts, change the members of an administrator account, or define the groups to which certain policies apply.

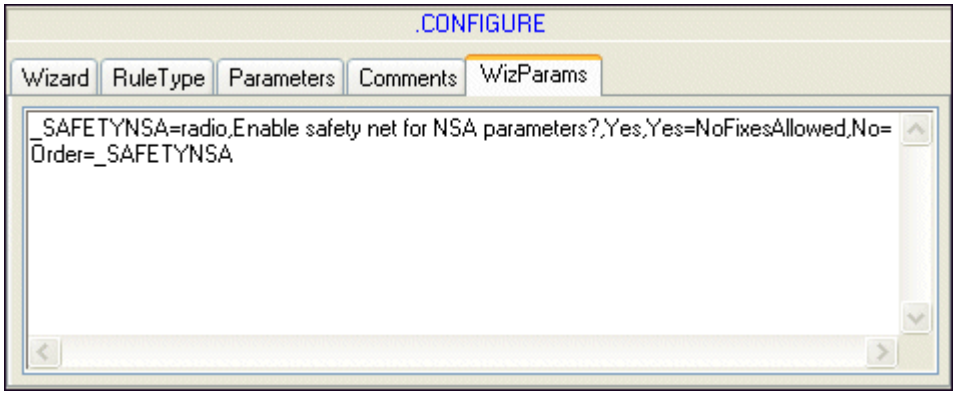
To understand the run-time policy variable, note the following settings in the NSA Guidelines for Windows XP and Windows 2000:

1. The name for the new rule must be .CONFIGURE.
2. The check type can be blank, or you can type CONFIGURE.

3. In the **Parameters** tab, the **Config** parameter is set to .CONFIGURE (Config=.CONFIGURE). When you set the Config key, the **WizParams** tab appears. On this tab you can type text using the WizParams syntax that controls the available text, input options, and parameters to modify in the **Wizard**.
4. View the **WizParams** tab to see the syntax that defines the Wizard's display for the rule. This example displays the question, "Enable safety net for NSA parameters?" In the **Wizard** you can select **Yes** or **No**.



The **Wizard** tab displays **MoreInfo** for this .CONFIGURE rule and the options defined in the Wizparams.



5. Review the **CrashOnAuditFull** rule in the **Parameters** tab. Note the **Modifiers** parameter, %get(.CONFIGURE:SAFETYNSA). The %get function calls the .CONFIGURE rule and uses the setting that enables the safety net setting for NSA parameters.

If you open the NSA Guidelines for Windows XP and Windows 2000 policy file, in the Preview pane you can click **Configure** to see the **Wizard** and the available options. If your policy file does not have a .CONFIGURE rule, the **Configure** link does not appear in the **Preview** pane.

Tip: This example describes how to use a .CONFIGURE rule in the console application. Rather than change the parameters there, you can select the variable settings in the server application and modify the .CONFIGURE rule. When you create a new Policy and select an associated policy file, the server application determines if a .CONFIGURE rule exists and displays prompts for

modifications. This rule may require synchronization between the database and the policy file. To synchronize the database and the new file, save the policy file in the database with a new name with new parameters for the .CONFIGURE rule, if previously saved in the database.

Notifications

Notifications

You can opt to receive email or program-output notifications when audits occur. Notifications apply to Audit-On-Schedule or Audit-On-Connect results and each audit can have one or more notification actions upon completion.

You may use notifications created in SecurityExpressions console in addition to the ones created in SecurityExpressions server. This application lets you select notifications created in both applications in the Schedules Tasks page and the Scopes page.

The Notifications table displays the notification Name, Type, and Values. From this page you create an email or command notification that you can edit or delete.

Creating New Command Notifications

To create a new command notification:

1. Click **Add New**.
2. Provide a **Notification Name**, a customized name of the notification to appear in the table.
3. Select Command as the **Type**.
4. Type the Command to run, which may be a URL. Include the command Arguments. You can pass variables to the command.

   If the command is a program, programs expect dependent files to be in the \system32\ folder.

5. Click **Add New**.

Creating New Email Notifications

When you create an email notification, you must identify the SMTP email server and the address from which the email should be sent.

To create a new email notification:

1. Click **Add New**.
2. Provide a Notification Name, a customized name of the notification to appear in the table.
3. Select Email as the Type.
4. Complete the following email information:

   To – person receiving the notification. This address appears as the Value in the table. Or Select allows you to select a previously entered email address.

   Subject – Notification topic. Or Select allows you to select a previously entered subject.

   Message – Text of the email notification, including variables.

   Examples: An audit has finished: %COMPUTER%

The group posture result is %GROUPPOSTURERESULT%.

Click here for the report: %RESULTLINK%

5. Select **Attach trace route information for Audit-on-Connect** for the message body to include the trace route. The message body always includes a link to the report for the audit that caused this notification.
6. **Recommended:** Click **Send Test** to make sure the notification will send as configured.
7. Click **Add New.**

Set Server for Email Notifications

Email notifications require that you set the SMTP server settings. These global settings include the email server (the name of the server through which to send email notifications) and the sender address (the email address of the person sending the email notifications).

Editing Notifications

To edit a Notification, click the Edit hyperlink on the Notifications table to select the row to edit. Make the necessary modifications and click **Update**.

To Edit an email notification, make the necessary modifications to:

- Notification Name
- To – person receiving the notification. This address appears as the Value in the table.
- Subject – Notification topic
- Message – Text of the email notification, including variables.
    - Check or clear the **Attach trace route information for Audit-on-Connect** box to determine whether or not the message body will include the trace route.

 We recommend you click **Send Test** to make sure the modified notification will send.

To Edit a command notification, make the necessary modifications to:

- Notification Name
- Command
- Optional Arguments

Deleting Notifications

Creating New Command Notifications

To create a new command notification:

1. Click **Add New** in the Notifications page.
2. Provide a Notification Name, a customized name of the notification to appear in the table.
3. Select **Command** as the Type.
4. Type the Command to run, which may be a URL. Include the command Arguments. You can pass variables to the command.

 If the command is a program, programs expect dependent files to be in the \system32\

folder.

5. Click **Add New**.

Creating New Email Notifications

To create a new email notification:

1. Click **Add New**.
2. Provide a Notification Name, a customized name of the notification to appear in the table.
3. Select Email as the Type.
4. Complete the following email information:

   To – person receiving the notification. This address appears as the Value in the table. Or Select allows you to select a previously entered email address.

   Subject – Notification topic. Or Select allows you to select a previously entered subject.

   Message – Text of the email notification, including variables.

   Examples: An audit has finished: %COMPUTER%

   The group posture result is %GROUPPOSTURERESULT%.

   Click here for the report: %RESULTLINK%

5. Select **Attach trace route information for Audit-on-Connect** for the message body to include the trace route. The message body always includes a link to the report for the audit that caused this notification.
6. **Recommended:** Click **Send Test** to make sure the notification will send as configured.
7. Click **Add New.**

Deleting Notifications

Click the **Delete** hyperlink for the notification that you want to remove. When you delete a notification, you remove it from the database. A warning appears to remind you that you are about to delete a record from the database. At this time, you can cancel the action or delete the record.

Notification Variables

You can include the variables listed here in any text-entry setting in a notification.

%RESULTLINK% - URL of the results or report

%POLICY% - policy used to perform the audit

%DESCRIPTION% - description of the task that executed the audit, from the Description box located in the Task Options and Scheduling dialog box's List tab


To learn more about the Task Options and Scheduling dialog box, check the SecurityExpressions Console help.

%DATE% - the date this task ran

The following three variables will only return a value if statistics are available:

%COUNTPROBLEMS% - number of errors encountered during the audit

%COUNTRULES% - number of rules used to audit the machine list

%SCORE% - the overall score resulting from the audit

The following four variables will only return a value if the task only audited one system:

%IP% - IP address or name of the system being audited, depending which represents the system in the machine list

%COMPUTER% - identical to the %IP% variable

%HOST% - identical to the %IP% variable

%GROUPPOSTURERESULT% - posture result of the system being audited

Example

A Subject or Message may contain text such as "Latest SecurityExpressions audit located at %RESULTLINK%."

My Machine Lists

My Machine Lists

When you schedule an audit task, you need to indicate which systems on the network you want the task to audit. The way to do that is to compile a machine list. A machine list collects in one place the names of the systems you want to audit in one session. Once you compile one or more machine lists, you can assign them to audit tasks.

In machine lists, systems are indicated by their system name or IP address. A machine list might include all systems in an organization, a department, a geographic territory, domain, or the entire network.

From the My Machine Lists page you add, edit, or delete a machine list. These machine lists, unlike any machine lists created in the console application (global machine lists), are secure personal lists. You must be logged in as the same user that created a list in order to use it, unless you belong to a Windows User Group listed in the Edit Private Items field in the Item Rights options.

Tip: When you schedule an audit, you can use either the machine lists created on this page or machine lists created in the console application (global machine lists). If all the machine lists you want to use were already created in the console, you do not have to create any machine lists here.

The table at the top of the My Machine Lists page contains the following information:

Column	Description
Edit	Click this link to edit the machine list in this row.
Delete	Click this link to delete the machine list in this row.
Name	Name of the machine list.
Member Count	The number of systems that are members of this machine list.

Windows Group Use Access	Windows User Groups who can use this machine list.
Windows Group Results Access	Windows User Groups who can view results from audits using this machine list.

Adding Machine Lists

To create a machine list:

1. Click the **Audit-On-Schedule** tab and then the **My Machine Lists** link.
2. Click the **Add** button to create a machine list.

   The Add/Update settings appear below the table.
3. In the List Name box, type a name for the machine list.
4. In the List Members box, type the names or IP addresses of all systems you want to add to the machine list. Type one name or address per line.

   Make sure you type the system names or IP addresses correctly. If you did not type a system's name or address correctly or somehow entered an invalid system, the audit skips the system and moves on to the next system in the list.
5. Set Windows Group Access. Enter Windows groups, separated by a comma, that can use this machine list and view audit results for it. This establishes which users can access this machine list and its audit results because of their role. If a Windows User Group isn't on the local computer, you'll need to enter the group in *domain**groupname* format.

   In the Use Machine List field, enter the Windows groups that should be able to use the machine list in scheduled audits. In the View Audit Results field, enter the Windows groups that should be able to view results from audits using the machine list. To grant all users access, type **Everyone**. To restrict all users, type **None**.
6. When you're done entering systems to add to the machine list, click the **Add/Update** button.

   The new machine list appears in the table at the top of the page.

Now you can add this machine list to a scheduled task.

Editing Machine Lists

To edit a machine list:

1. Click the **Audit-On-Schedule** tab and then the **My Machine Lists** link.
2. In the table at the top of the My Machine Lists page, click the **Edit** hyperlink in the same row as the machine list you want to edit.

   The Add/Update settings appear below the table. Make the necessary changes.
3. If you want to rename the machine list, type a new name in the List Name box.
4. If you want to add a system to the machine list, type its name or IP address on its own line in the List Members box. If you want to remove a system from the list, delete it.

Make sure you type the system names or IP addresses correctly. If you did not type a system's name or address correctly or somehow entered an invalid system, the audit skips the system and moves on to the next system in the list.

5. Set Windows Group Access. Enter Windows groups, separated by a comma, that can use this machine list and view audit results for it. This establishes which users can access this machine list and its audit results because of their role. If a Windows User Group isn't on the local computer, you'll need to enter the group in *domain**groupname* format.

   In the Use Machine List field, enter the Windows groups that should be able to use the machine list in scheduled audits. In the View Audit Results field, enter the Windows groups that should be able to view results from audits using the machine list. To grant all users access, type **Everyone**. To restrict all users, type **None**.

6. When you're done modifying the machine list, click the **Add/Update** button.

   The machine list appears in the table at the top of the page.

Deleting Machine Lists

Click the **Delete** hyperlink in the same row as the machine list that you want to delete. When you delete a machine list, you remove it from the database. A warning appears to remind you that you are about to delete a record from the database. At this time, you can cancel the action or delete the record.

Editing Global Machine Lists

You can use global machine lists, which are database machine lists created in the console application, to indicate which target systems you want to audit on a schedule. If a database machine list requires credentials in order to access the systems in it, and you plan to use it in the server application, someone needs to delegate the machine list's credentials to the server application.

To delegate a database machine list's credentials to the server application, open the console application, right click the Database Machine List in the Audit tab's left pane and select **Edit** from the menu. The Edit Machine List dialog box appears. Use the Connect tab and the Delegation tab to set and delegate credentials. For more information on editing machine lists in the console application, check its on-line help.

Scheduled Tasks

Scheduled Tasks

SecurityExpressions automatically starts a scheduled task at some future time based on options defined through Audit-On-Schedule.

Audit-On-Schedule specifies a daily, weekly, or monthly schedule to audit certain devices and how to audit those devices. You can assign previously created notifications to scheduled audits. While viewing the scheduled audits, you can click **Run Now** to run the task immediately.

From the Scheduled Task page you add, edit, or delete a task. You must be logged in as the same user that created a scheduled task in order to use it, unless you belong to a Windows User Group listed in the Edit Private Items field in the Item Rights options.

Scheduled tasks use only the policy file and .CONFIGURE information of a policy, ignoring the other settings.

The Scheduled Tasks table contains the following information:

Column	Description
Run Now/Stop/Initializing	Click this button to start or stop the task in this row. This column also displays "Initializing" when a task is in the middle of a process.
Edit	Click this link to edit the task in this row.
Delete	Click this link to delete the task in this row.
Description	A description of this task, created when you scheduled the task.
Machine Lists	Machine Lists to audit. All devices in all Machine Lists listed will be audited. You can only edit global Machine Lists in the SecurityExpressions Console.
Policies	Name of the Policies to use for the audit.
Run On	Server on which to run audit.
Last Ran	Last time this task ran.
Current Schedule	Time and frequency of the scheduled task.
Notifications	List of notifications to run when the task completes.
Windows Group Edit Access	Windows User Groups who can modify this task.
Windows Group Run Access	Windows User Groups who can use this task to run audits.
Hosts	How many computers were included in the most recently ran or currently running audit. This would be the total number of computers in all machine lists selected for the audit.
Done	How many computers were audited or had an audit attempt during the most recently ran or currently running audit.
Successful	How many computers were successfully audited during the most recently ran or currently running audit.
Connection Error	How many computers were not audited due to a connection error during the most recently ran or currently running audit.
Not Found	How many computers were not audited because they weren't found on the network during the most recently ran or currently running audit.

Adding Scheduled Tasks

To configure a new scheduled task:

1. Click the **Audit-On-Schedule** tab and then the **Scheduled Tasks** link.
2. Click the **Add New** button to configure a new task.

Basic Settings

3. In the Description box, type a brief statement identifying the scheduled task.

4. In the Policies list, select one or more policies on which you want to base any audits this task performs.

Policies are configured on the Policies page. If none of the existing policies meet your needs, you can configure a new one by clicking the **Edit Policy List** link, which opens the

Policies page.

Only the policies to which you have Use access rights appear for selection. Access rights for individual policies are set in the Windows Group Access options on the Policies page. If you can't find a policy you need to use, ask the policy's creator to add you to one of the Windows User Groups with Use access rights to the policy.

5. Select which machine list(s) you want to audit every time this task runs.

You may select any combination of machine lists from the Global Machine Lists, My Machine Lists, and Other User's Shared Machine Lists sections.

Only the machine lists to which you have Use access rights appear for selection. Access rights are set in the Windows Group Access options on the My Machine Lists page and the ML Access page (global machine lists). If you can't find a machine you need to use, ask the machine list's creator or administrator to add you to one of the Windows User Groups with Use access rights to the machine list.

- The Global Machine Lists section displays all machine lists in the SecurityExpressions Console, if your organization uses the console.

If the SecurityExpressions Console's database does not contain any machine lists, this section won't contain any machine lists.

- If you created any machine lists on the My Machine Lists page using the same user account as the one you're using to create this task, the My Machine Lists section displays those machine lists.

If the My Machine Lists page does not contain any machine lists created using the same user account as the one you're using to create this task, this section won't contain any machine lists.

- If anyone created any machine lists on the My Machine Lists page using a different user account than the one you're using to create this task, and entered a Windows User Group in the Use Machine List field that you're a member of, the Other User's Shared Machine Lists section displays those machine lists.

If the My Machine Lists page does not contain any machine lists that 1) were created using a different user account than the one you're using to create this task and 2) contain a Windows User Group in the Use Machine List field that you're a member of, this section won't contain any machine lists.

6. In the Server to Run On drop-down list, select which server you want run the task.

You can install the server software on more than one server system, as long as they all connect to one central database. Each server can have its own settings. Based on the way each server is configured, you'll want to use one particular server to perform the audits executed by this task, depending on your goals.

Schedule Settings

7. Select to run this task once, weekly, monthly, or not at all.

Not Scheduled - Lets you create a scheduled task without enabling it, or disable an existing scheduled task without deleting it.

Run Once – The scheduled task executes once on this day and does not repeat. In the calendar, choose the date on which you want to run the task.

Run Weekly – The task executes once every week on the day(s) you select. Check the days of the week on which you want to run the task.

Run Monthly – The task executes only during the months you select on the date you select.

8. In the Run At options, select the time of day at which you want to launch the task from the hour and minutes drop-down lists.

Make sure you select the correct hour, whether it's a.m. or p.m.

If you selected Not Scheduled in the previous step, these options don't appear.

Notifications

9. If you want to send notifications when this scheduled task executes, select one or more notifications from the Notifications list or the Console Notifications list.

The Notifications list contains the notifications created using the Notifications page in this application. If none of the existing notifications meet your needs, you can configure a new one by clicking the **Edit Notifications** link, which opens the Notifications page.

The Console Notifications list contains notifications created using the console application.

10. If you have Altiris Notification Server and you want to send information about the audits generated on this schedule to Notification Server, select **Send a Notification Server Event**. If you prefer to send this information after each target computer is audited, select **Send a Notification Server Event for each target**.

Hosts Not Connected Settings

11. If you want to enable Audit-on-Connect for any systems that could not be contacted on the first try, check the **Enable host audit on connect** box.

Between the initial connection failure and the next time the scheduled task runs, these systems get audited if they connect to the network. In this case, the task only completes after all systems connect.

In order for this feature to work on a target system, you need to create an Audit-on-Connect scope that includes that system.

12. If you want to continue to attempt auditing systems that could not be contacted on the first try, check the **Automatically re-audit devices that could not be contacted** box.

A. In the Wait this Many Minutes Before Retries box, type the number of minutes you want the task to wait before attempting a reaudit after a failed connection. After each round of audits, the task waits this length of time before reauditing systems that weren't available the first time.

This gives the system time to make itself available for connection. If you suspect system restarts might cause failed connections, for example, enter a length of time longer than a

restart would take.

B. If you want to set a time limit on how long the task can attempt reaudits, type the number of hours you want to allot for reaudits in the Attempt re-audit for this many hours after initial audit box.

A reaudit cycle could go on indefinitely if a system is off or never connects. Setting a time limit keeps the reaudit cycle from continuing indefinitely.

C. If you want to limit the amount of times the task can attempt to reaudit, type the number of reaudit attempts you'll allow in the Maximum number of attempts to re-audit box.

A reaudit cycle could go on indefinitely if a system is off or never connects. Limiting the number of times the task can attempt to reaudit systems keeps the reaudit cycle from continuing indefinitely.

Both steps B and C provide end points to the reaudit cycle. You may use one method or the other, or both. If you use both methods together, whichever limit is reached first ends the audit cycle.

Tip: Steps 11 and 12 each provide a way for audits to occur on systems that were not available when the task was scheduled to audit them. You may use these features together or separately. If you use them together, Audit-on-Connect is active both during and after the reaudit cycle.

If a system was contacted but the login credentials were incorrect, the task does not attempt to reaudit the system.

Other Options Settings

13. If you want to limit the length of time this task takes to complete from the time it actually begins auditing, regardless of the reason, click the **Limit to Hours** radio button in the Maximum amount of time an audit may run section. Then type the number of hours to which you want to limit the task.

After this number of hours, the task finishes auditing the system it was working on and then terminates. If reauditing or Audit-on-Connect on Fail is part of the task, they are included as part of the overall time it takes to run the entire task.

14. If you want to keep track of which target systems the task could not audit, check **Enable** in the Save target names that could not be contacted to the following machine list section. Then type a name for the machine list, using variables in the name if you want.

The machine list you enter saves the names of all systems that did not get audited as a result of the termination. Auditing this machine list later enables you to finish auditing the remaining systems.

If you type the name of an existing machine list, any systems already listed in it will be removed. Unless you want the machine list altered in the case of an incomplete audit, we recommend creating a database machine list expressly for this purpose.

Credentials Settings

15. If you want to use specific credentials to access all systems whenever this audit task runs, type those credentials in the Login box.

 If you do not want to specify credentials, skip to step 18.

16. In the Password box, type the password of the credentials you specified in the previous step.

17. If you want to make sure these credentials are used to access target systems instead of any credentials that might be delegated from other credential stores or from the console application, check the **Always use my credentials over delegated ones** box.

Windows Group Access

18. Set Windows Group Access. Enter Windows groups, separated by a comma, that can edit this scheduled task and use it to perform audits. This establishes which users can access this task and its audit results due to their role. If a Windows User Group isn't on the local computer, you'll need to enter the group in *domain**groupname* format.

In the Edit Task field, enter the Windows groups who should be able to modify the task. In the Run Task field, enter the Windows groups who should be able to use the task to perform audits. To grant all users access, type **Everyone**. To restrict all users, type **None**.

19. Click the **Add New** button to create this scheduled task.

Now the task appears in the table at the top of the Scheduled Tasks page.

Editing Scheduled Tasks

You can edit the tasks you created, plus any task created by someone else who selected the **Allow others to edit this task** option.

Note: You can view tasks created by someone else who did not opt to allow others to edit the task. You cannot make changes to them, however.

To edit a scheduled task:

1. Click the **Audit-On-Schedule** tab and then the **Scheduled Tasks** link.
2. In the table at the top of the Scheduled Tasks page, click the **Edit** hyperlink in the same row as the task you want to edit.

The Edit Task options appear. Make the necessary changes.

Basic Settings

3. In the Description box, type a brief statement identifying the scheduled task.

4. In the Policies list, select one or more policies on which you want to base any audits this task performs.

Policies are configured on the Policies page. If none of the existing policies meet your needs, you can configure a new one by clicking the **Edit Policy List** link, which opens the Policies page.

5. Select which machine list(s) you want to audit every time this task runs.

You may select any combination of machine lists from the Global Machine Lists, My Machine Lists, and Other User's Shared Machine Lists sections.

Only the machine lists to which you have Use access rights appear for selection. Access rights are set in the Windows Group Access options on the My Machine Lists page and the ML Access page (global machine lists). If you can't find a machine you need to use, ask the machine list's creator or administrator to add you to one of the Windows User Groups with Use access rights to the machine list.

- The Global Machine Lists section displays all machine lists in the SecurityExpressions Console, if your organization uses the console.

If the SecurityExpressions Console's database does not contain any machine lists, this section won't contain any machine lists.

- If you created any machine lists on the My Machine Lists page using the same user account as the one you're using to create this task, the My Machine Lists section displays those machine lists.

If the My Machine Lists page does not contain any machine lists created using the same user account as the one you're using to create this task, this section won't contain any machine lists.

- If anyone created any machine lists on the My Machine Lists page using a different user account than the one you're using to create this task, and entered a Windows User Group in the Use Machine List field that you're a member of, the Other User's Shared Machine Lists section displays those machine lists.

If the My Machine Lists page does not contain any machine lists that 1) were created using a different user account than the one you're using to create this task and 2) contain a Windows User Group in the Use Machine List field that you're a member of, this section won't contain any machine lists.

6. In the Server to Run On drop-down list, select which server you want run the task.

You can install the server software on more than one server system, as long as they all connect to one central database. Each server can have its own settings. Based on the way each server is configured, you'll want to use one particular server to perform the audits executed by this task, depending on your goals.

Schedule Settings

7. Select to run this task once, weekly, monthly, or not at all.

Not Scheduled - Lets you create a scheduled task without enabling it, or disable an existing scheduled task without deleting it.

Run Once – The scheduled task executes once on this day and does not repeat. In the calendar, choose the date on which you want to run the task.

Run Weekly – The task executes once every week on the day(s) you select. Check the days of the week on which you want to run the task.

Run Monthly – The task executes only during the months you select on the date you select.

8. In the Run At options, select the time of day at which you want to launch the task from the hour and minutes drop-down lists.

Make sure you select the correct hour, whether it's a.m. or p.m.

If you selected Not Scheduled in the previous step, these options don't appear.

Notifications

9. If you want to send notifications when this scheduled task executes, select one or more notifications from the Notifications list or the Console Notifications list.

The Notifications list contains the notifications created using the Notifications page in this application. If none of the existing notifications meet your needs, you can configure a new one by clicking the **Edit Notifications** link, which opens the Notifications page.

The Console Notifications list contains notifications created using the console application.

10. If you have Altiris Notification Server and you want to send information about the audits generated on this schedule to Notification Server, select **Send a Notification Server Event**. If you prefer to send this information after each target computer is audited, select **Send a Notification Server Event for each target**.

Hosts Not Connected Settings

11. If you want to enable Audit-on-Connect for any systems that could not be contacted on the first try, check the **Enable host audit on connect** box.

Between the initial connection failure and the next time the scheduled task runs, these systems get audited if they connect to the network. In this case, the task only completes after all systems connect.

In order for this feature to work on a target system, you need to create an Audit-on-Connect scope that includes that system.

12. If you want to continue to attempt auditing systems that could not be contacted on the first try, check the **Automatically re-audit devices that could not be contacted** box.

A. In the Wait this Many Minutes Before Retries box, type the number of minutes you want the task to wait before attempting a reaudit after a failed connection. After each round of audits, the task waits this length of time before reauditing systems that weren't available the first time.

This gives the system time to make itself available for connection. If you suspect system restarts might cause failed connections, for example, enter a length of time longer than a restart would take.

B. If you want to set a time limit on how long the task can attempt reaudits, type the number of hours you want to allot for reaudits in the Attempt re-audit for this many hours after initial audit box.

A reaudit cycle could go on indefinitely if a system is off or never connects. Setting a time limit keeps the reaudit cycle from continuing indefinitely.

C. If you want to limit the amount of times the task can attempt to reaudit, type the number of reaudit attempts you'll allow in the Maximum number of attempts to re-audit box.

A reaudit cycle could go on indefinitely if a system is off or never connects. Limiting the number of times the task can attempt to reaudit systems keeps the reaudit cycle from continuing indefinitely.

Both steps B and C provide end points to the reaudit cycle. You may use one method or the other, or both. If you use both methods together, whichever limit is reached first ends the audit cycle.

Tip: Steps 11 and 12 each provide a way for audits to occur on systems that were not available when the task was scheduled to audit them. You may use these features together or separately. If you use them together, Audit-on-Connect is active both during and after the reaudit cycle.

If a system was contacted but the login credentials were incorrect, the task does not attempt to reaudit the system.

Other Options Settings

13. If you want to limit the length of time this task takes to complete from the time it actually begins auditing, regardless of the reason, click the **Limit to Hours** radio button in the Maximum amount of time an audit may run section. Then type the number of hours to which you want to limit the task.

After this number of hours, the task finishes auditing the system it was working on and then terminates. If reauditing or Audit-on-Connect on Fail is part of the task, they are included as part of the overall time it takes to run the entire task.

14. If you want to keep track of which target systems the task could not audit, check **Enable** in the Save target names that could not be contacted to the following machine list section. Then type a name for the machine list, using variables in the name if you want.

The machine list you enter saves the names of all systems that did not get audited as a result of the termination. Auditing this machine list later enables you to finish auditing the remaining systems.

If you type the name of an existing machine list, any systems already listed in it will be removed. Unless you want the machine list altered in the case of an incomplete audit, we recommend creating a database machine list expressly for this purpose.

Credentials Settings

15. If you want to use specific credentials to access all systems whenever this audit task runs, type those credentials in the Login box.

If you do not want to specify credentials, skip to step 18.

16. In the Password box, type the password of the credentials you specified in the previous step.

17. If you want to make sure these credentials are used to access target systems instead of any credentials that might be delegated from other credential stores or from the console application, check the **Always use my credentials over delegated ones** box.

Windows Group Access

18. Set Windows Group Access. Enter Windows groups, separated by a comma, that can edit this scheduled task and use it to perform audits. This establishes which users can access this task and its audit results due to their role. If a Windows User Group isn't on the local computer, you'll need to enter the group in *domain**groupname* format.

In the Edit Task field, enter the Windows groups who should be able to modify the task. In the Run Task field, enter the Windows groups who should be able to use the task to perform audits. To grant all users access, type **Everyone**. To restrict all users, type **None**.

19. Click the **Update** button to create this scheduled task.

The updated task appears in the table at the top of the Scheduled Tasks page.

Deleting Scheduled Tasks

Click the **Delete** hyperlink in the same row as the scheduled task that you want to delete. When you delete a scheduled task, you remove it from the database. A warning appears to remind you that you are about to delete a record from the database. At this time, you can cancel the action or delete the record.

View Audit-On-Connect Activity

Browse Audit-On-Connect Activity

Audit-On-Connect activity reports show Audit-On-Connect connection events as they were logged over time. Use these reports to troubleshoot and optimize Audit-on-Connect configurations.

SecurityExpressions Audit & Compliance Server dynamically generates reports based on preconfigured or user-defined report profiles. When you first browse Audit-On-Connect activity, a table appears with Audit-On-Connect preconfigured reports and any previously created user-defined reports. SecurityExpressions Audit & Compliance Server provides five Audit-On-Connect preconfigured reports, which are status reports over specific time periods. The top level table shows names such as Status 01 Hour as a preconfigured report. Additional standard reports include Audit-On-Connect Error Log and Audit-On-Connect Exceptions.

Click **Show** to open the saved report profile. Click **Details** to drill-down to see details.

 Only the policies and scopes to which you have Use access rights appear for selection. Access rights are set in the Windows Group Access options on the Policies page and Scopes page. If you can't find a policy or scope you need to use, ask the item's creator or administrator to add you to one of the Windows User Groups with Use access rights to it.

Furthermore, reports only display audit results involving scopes to which you have View access rights and policies to which you have Result access rights.

Audit-On-Connect Activity Table

Column	Description
Preconfigured	**Yes** indicates a standard report. **No** indicates a custom report profile.
Name	Report Name from the Audit-On-Connect Activity Report Profile
Description	Report description from the Audit-On-Connect Activity Report Profile
Show Most Recent	If you audit the same device multiple times, show the most recent activity report
Detection Methods	Connection Monitor type, which includes DHCP, EventLog, or both
Date From	Date and time activity reporting started
Date To	Date and time activity reporting ended

Adding a New Audit-On-Connect Report Profile

Creating a new report profile creates a filter for a report and defines what appears in each report.

To define a new Audit-On-Connect Report Profile, click **New** and save the settings and fields to include in the report.

1. Type a **Report Name** and a short report **Description**.

2. Select one or more **Detection Methods**. The detection method identifies the Connection Monitor types.
3. Define filters that cause only certain events that meet your criteria to display in the report. Click the links and set the criteria. You may set as many kinds of filters as you like. The report's contents are based on a combination of all filters you set.

Note: When you click a new link, the options from the previous link no longer display but any options you selected there are still selected. To help you remember which links have filters selected, a check mark appears next to them.

Group Posture Results - Select as many as you want.

Device Type - Select as many as you want.

Enter MACs - Type the MAC addresses you want to use as criteria. One per line.

Enter IP Addresses - Type the IP addresses you want to use as criteria. One per line.

Enter Device Name - Type the device names you want to use as criteria. One per line.

Scope Name – Select as many as you want. More than one Policy can apply to a Scope. If you do not filter by policy, all data displays.


If a computer is listed in multiple scopes, the only Windows Group Access settings that apply to the audit results are the ones from the scope used by the audit.

4. In the **Show Fields** section, check the boxes to choose which additional columns you want to appear in the summary report of this profile.

5. Under **Date/Hour Range Selection**, select one of the following options and set a range of data to display each time the report runs.

- Open or closed range beginning on a specific day - Includes in the report a range of connection activity starting on a specific date. You may specify an end for the date range or let the report display all activity available after the starting date.
- Relative range from the current date - Includes in the report a range of connection activity prior to the day the report ran. Enter how many days, hours and minutes worth of prior data you want to display in the report.

6. Select **Most Recent Audit** to show the most recent audit only and remove duplicate data.

7. Click **Save** to save this report profile.

Editing Report Profiles

To edit a report profile, click the Edit hyperlink and modify the same settings as during the profile creation.

Deleting Report Profiles

To delete a report profile:

1. Click the Edit hyperlink on the Browse Audit-On-Connect Activity table to select the report profile to remove.

2. When you delete a report profile, you remove it from the database. A warning appears to remind you that you are about to this particular report profile from the database. Cancel the action or delete the record.

Audit-On-Connect Error Log Report

The Audit-On-Connect Error Log Report displays the errors for each server at a specific time as they were written to the Windows error log.

Audit-On-Connect Exceptions Report

The Exceptions report shows the Audit-On-Connect Exceptions with a column that counts how often the exception processed.

View Audit Results

Browse Audit Results

This page shows audit results in the form of reports. It features results from almost all kinds of auditing methods, including:

- Audit-on-Schedule
- Audit-on-Connect
- self-service audits based on multiple policy files and Audit-on-Connect scopes
- audits performed on any consoles connected to the same database as the server application

SecurityExpressions Audit & Compliance Server dynamically generates reports based on pre-configured report profiles. Clicking a hyperlink drills down to a new page with a report showing all of the policy files and the individual policy file posture result used during the audit of the device. Additionally you can drill down by policy file to the audit detail for that audit. When browsing audit data, you may view it but cannot modify it.

When you first browse Audit-On-Schedule activity, a table appears with Audit-On-Schedule pre-configured reports and any previously created user-defined reports. SecurityExpressions Audit & Compliance Server provides one Audit-On-Schedule pre-configured report, which is a status report over 30 days, plus one additional standard report called Scheduled Audits Log.

Once you have created a report profile, you can drill down into the details of the report. Click **Show** to begin to see the which device was audited, by whom, the policy file used for the audit, and the results. Clicking **Details** from this Audit List displays the audit report with greater details. For example, you can see the status and priority for each rule.

 Only the machine lists, policies, scheduled tasks, and scopes (when viewing Audit-on-Connect results) to which you have Use access rights appear for selection. Access rights are set in the Windows Group Access options on the My Machine Lists page, ML Access page, Policies page, Scheduled Tasks page, and Scopes page. If you can't find a machine list, policy, scheduled task, or scope you need to use, ask the item's creator or administrator to add you to one of the Windows User Groups with Use access rights to it.

Furthermore, reports only display audit results involving scopes to which you have View access rights, policies to which you have Result access rights, and machine list members audited using machine lists to which you have Result access rights.

Adding a New Audit Results Report Profile

Creating a new report profile defines a report filter and what appears in each report.

1. Click the **New** button to display report-profile options.
2. Type a **Report Name** and a short report **Description**.
3. Select a report type and then define filters that cause only certain audit results that meet your criteria to display in the report.

   The filter options available depend on the report type you select.

- **Data Grid** - Generates a highly interactive HTML report with lots of opportunities to drill down. Click the links and set the criteria. You may set as many kinds of filters as you like. The report's contents are based on a combination of all filters you set.
  To learn more about the available filters, click here [click link again to close]

  Note: When you click a new link, the options from the previous link no longer display but any options you selected there are still selected. To help you remember which links have filters selected, a check mark appears next to them.

  Show Current Value - Check to add this column to the report.

  Show Description - Check to add this column to the report.

  Policy - Select as many as you want.

  Only the policies to which you have Use access rights appear for selection. Access rights are set in the Windows Group Access options on the Policies page. If you can't find a policy you need to use, ask the policy's creator to add you to one of the Windows User Groups with Use access rights to the policy.

  Scanned By - Select as many as you want.

  Scanned From - Select as many as you want.

  Computers in Machine List - Displays the names of all machine lists, including both database machine lists created in the console and My Machine Lists created in this application. Select as many as you want.

   Only the machine lists to which you have Use access rights appear for selection. Access rights are set in the Windows Group Access options on the My Machine Lists page and the ML Access page. If you can't find a machine list you need to use, ask the machine list's creator or administrator to add you to one of the Windows User Groups with Use access rights to the machine list. .

- **Crystal Report** - Generates a Crystal report with the standard features. Select the report format from the scroll box.

- **PDF** - Generates a PDF version of a Crystal report for easy transporting. Select the report format from the scroll box.

4. Select whether you want the report to include Audit-on-Schedule and Audit-on-Connect results or just Audit-on-Schedule results. In the Scheduled Audit Only list, select **Yes** for Audit-on-Schedule results only or **No** for both kinds of results.

5. In the Benchmark Score Less Than box, type the maximum score an audit must have in order for its results to display in the report. The results of any audit with a higher score than this will be considered not critical enough to appear in the report.

6. In the **Show Fields** section, check the boxes to choose which additional columns you want to appear in the summary report of this profile.

7. Under **Date/Hour Range Selection**, select one of the following options and set a range of data to display each time the report runs.

- Open or closed range beginning on a specific day - Includes in the report a range of connection activity starting on a specific date. You may specify an end for the date range or let the report display all activity available after the starting date.
- Relative range from the current date - Includes in the report a range of connection activity prior to the day the report ran. Enter how many days, hours and minutes worth of prior data you want to display in the report.

8. Select **Most Recent Audit** to show the most recent audit only and remove duplicate data.

9. Click **Save** to save this report profile.

Editing Audit Report Results Profiles

To edit the Audit Report Results Profile, click the Edit hyperlink and modify the settings established during the report profile creation.

Deleting Audit Report Results Profiles

To delete an Audit Report Results Profile:

1. Click the Edit hyperlink on the Browse Audit Results table to select the report profile to remove.
2. When you delete a report profile, you remove it from the database. A warning appears to remind you that you are about to this particular report profile from the database. Cancel the action or delete the record.

Scheduled Audits Log Report

The Scheduled Audits Log Report displays schedule errors as they were written to the Windows error log.

Adding Custom Reports to the Server Application

You can use reports created using Crystal Reports Designer in the server application if you add them to the server application in a new audit-results report profile.


You can only create reports if you have a full copy of Crystal Reports purchased and installed on the computer where the server application is installed. Contact customer support for advice on which version to obtain.

To add a custom report to the server application:

1. Create the report in Crystal Reports Designer, making sure to use the ScanStats table or any existing view whose name begins with "tempquery_."

   You must use either the ScanStats table or an existing view whose name begins with "tempquery_" for the report to work properly within the server application.
2. Copy the report to C:\Program Files\Altiris\Security Management\SecurityExpressions\seserver\reporting\crystal\. This path is different if you didn't install the server application in the default location.
3. In the Browse Audit Results page, create a new audit-results report profile, selecting Crystal Report as the report type.

Glossary

#

.CONFIGURE: Some policy files, such as the NSA Guidelines for Windows XP and Windows 2000, contains special rule named .CONFIGURE. The .CONFIGURE rule allows you to configure your policy files and set global parameters for policy files at run time.

A

Active Directory Connection Monitor: Connection monitor for Active Directory domains that detects computers coming on the network

Audit Service: Back-end Windows service that performs audits.

authentication: Authentication is any process by which a system verifies the identity of a user who wishes to access it.

C

Credential Store: Group of passwords securely stored in the database for a SecurityExpressions User

credentials: A set of Credentials is information used to verify the identity of a user. Normally a User ID and a Password, together, form a set of Credentials.

D

DNS: DNS is the Domain Name Service, a hierarchical global infrastructure deployed on the Internet and private IP-based networks used to resolve domain names into IP addresses.

E

Exceptions: A list of devices whose Group Posture is predetermined. An Exceptions list is an explicit list of devices to be excluded from an audit. Exceptions complement Scopes.

G

Generic DHCP Connection Monitor: The connection monitor/listener for DHCP Servers that detects computers coming on the network

I

Impact: Possible adverse impact of applying the rule. Suggested values are high, low, and normal, but you may specify any text. Impact may be a key in a rule.

M

Microsoft DHCP Server Connection Monitor: The connection monitor/plugin for Microsoft DHCP Servers that detects computers coming on the network

P

policy: A Security Policy is a set of objectives, rules of behaviour for users and administrators, and requirements for system configuration and management that collectively are designed to ensure Security of computer systems in an organization.

Priority: Importance of applying the rule. Priority may be a key in a rule.

proxy: A Windows computer running the Agent.

S

scheduled audit: Audit performed by the Scheduler service.

Scheduler: The program that performs Scheduled Audits.

SecurityExpressions Audit and Compliance Server: SecurityExpressions server including the Web front end, scheduler, and Audit-On-Connect back end.

SSH: SSH (Secure Shell) is a program to log into another computer over a network, to execute commands in a remote system, and to move files from one computer to another. It provides strong authentication and secure communications over insecure channels.

Index